USER MANUAL

AXIS Q6045–S PTZ Dome Network Camera

About this Document

This manual is intended for administrators and users of the AXIS Q6045–S PTZ Dome Network Camera, and is applicable to firmware 5.55 and later. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis website, as required. See also the product's online help, available via the web-based interface.

Legal Considerations

Video surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

This product includes one (1) H.264 decoder license. To purchase further licenses, contact your reseller.

Liability

Every care has been taken in the preparation of this document. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at *www.axis.com/patent.htm* and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see *www.opensource.apple.com/apsl*). The source code is available from *https://developer.apple.com/bonjour/*

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC and VAPIX are registered trademarks or trademark applications of Axis AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

Apple, Boa, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, Windows Vista and WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

SD, SDHC and SDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both. Also, miniSD, microSD, miniSDHC, microSDHC, microSDXC are all trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Regulatory Information

Europe

CE This product complies with the applicable CE marking directives and harmonized standards:

- Electromagnetic Compatibility (EMC) Directive 2004/108/EC. See *Electromagnetic Compatibility (EMC), on page 2*.
- Low Voltage (LVD) Directive 2006/95/EC. See *Safety, on page 3*.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU. See *Disposal and Recycling, on page 3*.

A copy of the original declaration of conformity may be obtained from Axis Communications AB. See *Contact Information, on page 3*.

Electromagnetic Compatibility (EMC)

This equipment has been designed and tested to fulfill applicable standards for:

- Radio frequency emission when installed according to the instructions and used in its intended environment.
- Immunity to electrical and electromagnetic phenomena when installed according to the instructions and used in its intended environment.

USA

This equipment has been tested using a shielded network cable (STP) and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The product shall be connected using a shielded network cable (STP) that is properly grounded.

Canada

This Class A digital apparatus complies with Canadian ICES-003. The product shall be connected using a shielded network cable (STP) that is properly grounded.

Cet appareil numérique de la classe A est confome à la norme NMB-003 du Canada. Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Europe

This digital equipment fulfills the requirements for RF emission according to the Class A limit of EN 55022. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

This product fulfills the requirements for emission and immunity according to EN 50121-4 and IEC 62236-4 railway applications.

This product fulfills the requirements for immunity according to EN 61000-6-1 residential, commercial and light-industrial environments.

This product fulfills the requirements for immunity according to EN 61000-6-2 industrial environments.

This product fulfills the requirements for immunity according to EN 55024 office and commercial environments

Australia/New Zealand

This digital equipment fulfills the requirements for RF emission according to the Class A limit of AS/NZS CISPR 22. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

Japan

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害 を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求され ることがあります。 本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

Korea

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다. 적절히 접지된 STP (shielded twisted pair) 케이블을 사용하여 제품을 연결 하십시오.

Safety
This product complies with IEC/EN 60950-1 and IEC/EN 60950-22, Safety of Information Technology Equipment. The product shall be grounded either through a shielded network cable (STP) or other appropriate method.

The power supply used with this product shall fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) according to IEC/EN/UL 60950-1.

The power supply used with this product shall fulfill the requirements for Safety Extra Low Voltage (SELV) according to IEC/EN/UL 60950-1.

Battery
The Axis product uses a 3.0 V BR/CR2032 lithium battery as the power supply for its internal real-time clock (RTC). Under normal conditions this battery will last for a minimum of five years.

Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product's server report. For more information about the server report, see the product´s setup pages or contact Axis support.

The battery should not be replaced unless required, but if the battery does need replacing, contact Axis support at *www.axis.com/techsup* for assistance.

⚠WARNING

- Risk of explosion if the battery is incorrectly replaced.
- Replace only with an identical battery or a battery which is recommended by Axis.
- Dispose of used batteries according to local regulations or the battery manufacturer's instructions.

Disposal and Recycling
When this product has reached the end of its useful life, dispose of it according to local raws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.

Europe

This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

This product complies with the requirements of Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

China

This product complies with the requirements of the legislative act Administration on the Control of Pollution Caused by Electronic Information Products (ACPEIP).

Contact Information
Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden

Tel: +46 46 272 18 00
Fax: +46 46 13 61 30

www.axis.com

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- download user documentation and software updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrase
- report problems to Axis support staff by logging in to your private support area
- chat with Axis support staff (selected countries only)
- visit Axis Support at *www.axis.com/techsup/*

Learn More!

Visit Axis learning center *www.axis.com/academy/* for useful trainings, webinars, tutorials and guides.

Table of Contents

Hardware Overview 6
- Connectors and Buttons 7
- LED Indicators 7
- Media Converter Switch 8
- Media Converter Switch Connectors 8
- Network Connector Dip Switches 9
- Media Converter Switch LED Indicators 10

Accessing the Product 11
- Access from a Browser 11
- Access from the Internet 12
- Set the Root Password 12
- The Live View Page 13

Media Streams 16
- How to Stream H.264 16
- MJPEG 16
- AXIS Media Control (AMC) 16
- Alternative Methods of Accessing the Video Stream 17

Setting Up the Product 19
- Basic Setup 19

Video 20
- Video Stream 20
- Stream Profiles 21
- Camera Settings 22
- Overlay 23
- Privacy Mask 24

Live View Config 26

PTZ (Pan Tilt Zoom) 29
- Preset Positions 29
- Gatekeeper 30
- Autotracking 30
- Guard Tour 31
- OSDI Zones 32
- Advanced 32
- Control Queue 33

Detectors 34
- Shock Detection 34
- Motion Detection 34
- Object Removed 35
- Enter/Exit Detector 36
- Fence Detector 36
- Object Counter 36

Applications 37
- Application Licenses 37
- Install Application 37
- Application Considerations 37

Events 39
- Setting Up an Action Rule 40
- Recipients 41
- Schedules 42
- Recurrences 43

Recordings 44
- Recording List 44
- Continuous Recording 44

Languages 45

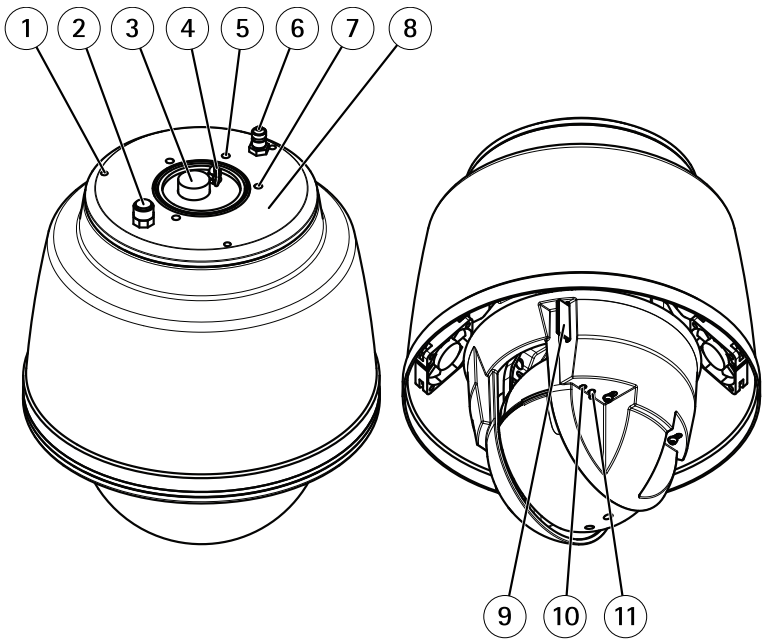
System Options 46
- Security 46
- Date & Time 48
- Network 48
- Storage 53
- Ports & Devices 55
- Maintenance 55

Table of Contents

Support 55
Advanced 56
Reset to Factory Default Settings 57
Multi-Connector Cable 58
Troubleshooting 59
Checking the Firmware 59
Upgrading the Firmware 59
Symptoms, Possible Causes and Remedial Actions 60
Technical Specifications 63
Media Converter Switch Connectors 66
Performance Considerations 67

Hardware Overview

Hardware Overview



1 *Mounting hole for sunshield (3x)*
2 *Pressure relief valve*
3 *Multiconnector*
4 *Hook for safety wire*
5 *Guide hole*
6 *Inlet valve*
7 *Mounting hole (3x)*
8 *Part number (P/N) & Serial number (S/N)*
9 *SD card slot (SDHC)*
10 *Status LED indicator*
11 *Control button*

Pressurize the Camera (Recommended)

The camera housing can be filled with Nitrogen gas to prevent condensation.

The filling process is repeated three times, releasing the pressure between fillings, to make sure that all air and humidity is purged from the housing.

Note

The camera housing has an pressure relief valve that limits the filling pressure to 0.5 bar (7 psi). During normal use the pressure inside the camera housing may drop below that pressure. For full protection make sure that the pressure is above 0.2 bar (3 psi) .

1. Set the regulator gauge on the gas cylinder to 0.5 bar (7 psi).
2. Remove the caps from the inlet valve and the pressure relief valve.
3. Place the chuck on the inlet valve and press down to fill the camera with nitrogen.
4. When the pressure inside the camera housing reaches 0.5 bar (7 psi) the pressure relief valve will open. Place your hand over the pressure relief valve to verify that the gas is flowing out.

Hardware Overview

5. Keep the gas flowing through the camera housing for one minute before removing the chuck from the inlet valve.
6. Lift the pressure relief valve to let the overpressure out of the camera unit.
7. Repeat the filling process a total of 3 times, leaving the the camera pressurized the last time.
8. Put the caps back on the inlet valve and the pressure relief valve.

Connectors and Buttons

For technical specifications, see *page 63*.

Multi-connector

Terminal connector for connecting the supplied media converter switch, which provides the following signals:

- DC Power
- Network (Ethernet 10/100Base-T)
- Input/Output (I/O)

The supplied multi-connector cable is required in order to maintain the product's IP rating, see *Multi-Connector Cable, on page 58*.

SD Card Slot

An SD card (not included) can be used for local recording with removable storage. For more information, see *Technical Specifications*.

NOTICE

To prevent corruption of recordings, the SD card should be unmounted before removal. To unmount, go to **Setup > System Options > Storage > SD Card** and click **Unmount**.

Control Button

The control button is used for:

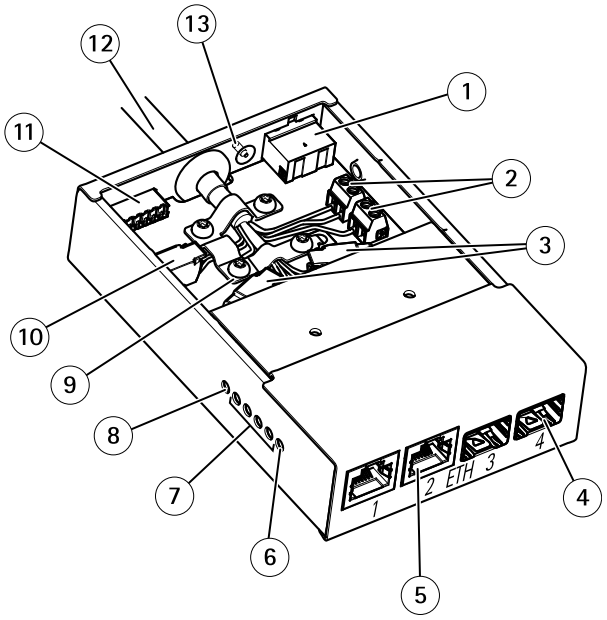
- Resetting the product to factory default settings. See *page 57*.
- Connecting to an AXIS Video Hosting System service. See *page 50*. To connect, press and hold the button for about 1 second until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See *page 50*. To connect, press and hold the button for about 3 seconds.

LED Indicators

LED	Color	Indication
Status	Unlit	Connection and normal operation
	Amber	Steady during startup. Flashes during firmware upgrade.
	Amber/red	Flashes amber/red if network connection is unavailable or lost.
	Red	Flashes red for firmware upgrade failure.
	Green	Shows steady green for 10 seconds for normal operation after restart.

Hardware Overview

Media Converter Switch



1 *Power connector (DC input)*
2 *Power connector (DC output)*
3 *Network connector (internal)*
4 *Network slot SFP (external) (2x)*
5 *Network connector RJ45 (external) (2x)*
6 *Camera LED indicator*
7 *Network LED indicator (4x)*
8 *Power LED indicator*
9 *Ground clip*
10 *I/O connector (internal)*
11 *I/O connector (external)*
12 *Multi-connector cable*
13 *Ground screw*

Media Converter Switch Connectors

For technical specifications, see *page 63*.

NOTICE

The product shall be connected using a shielded network cable (STP) or an optical fiber cable. All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements, see *Electromagnetic Compatibility (EMC), on page 2*.

Important

The media converter switch does not support hotswapping. Disconnect power from the switch before swapping cameras. An attempt to hotswap could cause the switch to freeze, in which case it must be restarted.

Power connector (DC input) – 2-pin terminal block for power input.

Power connector (DC output) – Two 2-pin terminal block for power output (pin 4 is not used).

Network connector RJ45 (external) – Two RJ45 connectors (10/100Base-T) for network connectivity.

Hardware Overview

Network slot SFP (external) – Two SFP slots (100Base-FX/1000Base-X) for network connectivity.

Each RJ45 and SFP port has its own dip switch. The dip switches control how the port forwards data. See *Network Connector Dip Switches*.

Dip switch position		Description of use
Default (middle)	B	When connecting to the network, directly or through a router or network switch.
Left	A	When connecting to a camera or a device that is not intended for viewing data.
Right	C	When connecting to another media converter switch.

Network connector (internal) – Two 2-pin Ethernet terminal blocks.

I/O connector (external) – 6-pin configurable I/O terminal block, which is connected to the camera through the multi-connector cable. Use with external devices in combination with, for example, tampering alarms, motion detection, event triggering, time lapse recording and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the I/O connector provides the interface to:

- **Digital output –** For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, output buttons on the Live View page or by an Action Rule. The output will show as active (shown under **System Options > Port & Devices > Port Status**) if the alarm device is activated.
- **Digital input –** An alarm input for connecting devices that can toggle between an open and closed circuit, for example: PIRs, door/window contacts, glass break detectors, etc. When a signal is received the state changes and the input becomes active (shown under **System Options > Port & Devices > Port Status**).

I/O connector (internal) – 2–pin I/O terminal block.

Network Connector Dip Switches

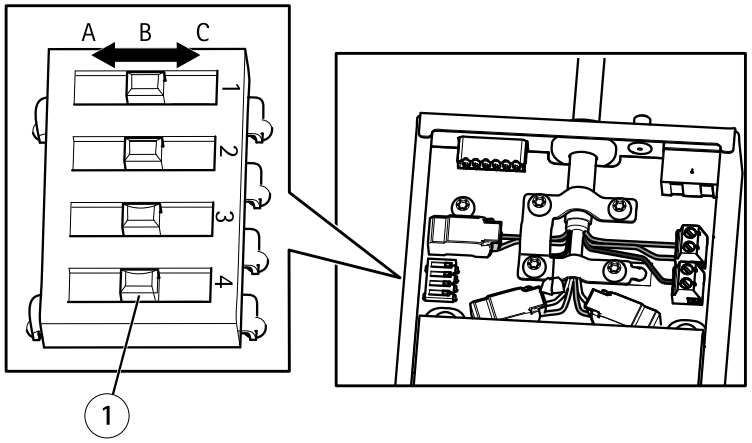
Important

Always use the default dip switch setting (position B) if the relationship between devices in the system is not defined.

The camera attaches a particular VLAN tag to all its forwarded multicast packages. The media converter switch manages how these multicast packages are forwarded between cameras, media converter switches and other network devices. This especially useful when connecting the camera and media converter switch to the network in a daisy chain.

By changing the position of the dip switches, each network connector port in the media converter switch can be configured to manage multicasts in three different ways.

Hardware Overview



Dip switch position		Description
Default (middle)	B	Remove VLAN tags from forwarded multicast packages. Use this setting when connecting to the network, directly or through a router or network switch.
Left	A	Block multicast packages that have a VLAN tag. Use this setting when connecting to a device that is not intended for multicast viewing.
Right	C	Forward multicast packages with a VLAN tag. Use this setting when connecting to another media converter switch.

VLAN tags are used to create independent logical networks, virtual local area networks (VLANs), within a physical network. Multiple media converter switches that are connected to each other in a daisy chain are members of the same VLAN. The media converter switches tag the multicast packages moving between them so that the next media converter switch in line knows the destination of the packages. In other words, the VLAN tag serves as a VLAN identifier. VLAN tagging should only be used when using multiple cameras and media converter switches because forwarding multicast packages with a VLAN tag only serves a purpose when the port is connected to another media converter switch, which might be connected to potential viewers.

Note

When connecting an outgoing media converter switch network connector to another type of network device, set the dip switch to position A to protect the device from multicast traffic.

Media Converter Switch LED Indicators

LED	Color	Indication
Power	Unlit	DC power unconnected or current protection engaged (power overload)
	Green	DC power connected.
Network (4x)	Amber	10 Mbit connection. Flashes during activity.
	Green	100/1000 Mbit connection. Flashes during activity.
Camera	Green	100 Mbit connection. Flashes during activity.

Accessing the Product

Accessing the Product

To install the Axis product, refer to the Installation Guide supplied with the product.

The product can be used with most operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications, on page 63*.

To view streaming video in Internet Explorer, allow installation of AXIS Media Control (AMC) when prompted.

The Axis product includes one (1) H.264 decoder license for viewing video streams. The license is automatically installed with AMC. The administrator can disable the installation of the decoders, to prevent installation of unlicensed copies.

Note

- QuickTime™ is also supported for viewing H.264 streams.
- If your computer restricts the use of additional software components, the product can be configured to use a Java applet for viewing Motion JPEG.

Access from a Browser

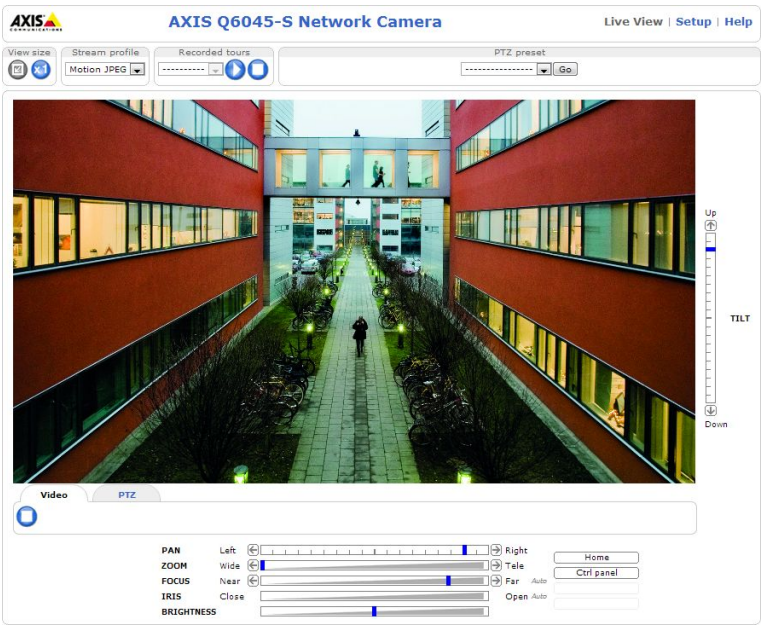
1. Start a browser (Internet Explorer, Firefox, Safari).
2. Enter the IP address or host name of the Axis product in the browser's Location/Address field. To access the product from a Macintosh computer (Mac OS X), click on the Bonjour tab and select the product from the drop-down list.

   If you do not know the IP address, use AXIS IP Utility to locate the product on the network. For information about how to discover and assign an IP address, see the Installation and Management Software CD or the document *Assign an IP Address and Access the Video Stream* on Axis Support web at www.axis.com/techsup
3. Enter your user name and password. If this is the first time the product is accessed, the root password must first be configured. For instructions, see *Set the Root Password, on page 12*.
4. The product's Live View page opens in your browser.

Note

The controls and layout of the Live View page may have been customized to meet specific installation requirements and user preferences. Consequently, some of the examples and functions featured here may differ from those displayed in your own Live View page.

Accessing the Product



Access from the Internet

Once connected, the Axis product is accessible on your local network (LAN). To access the product from the Internet you must configure your network router to allow incoming data traffic to the product. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the product. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.

For more information, see *NAT traversal (port mapping) for IPv4, on page 51*. See also AXIS Internet Dynamic DNS Service at *www.axiscam.net*

For Technical notes on this and other topics, visit the Axis Support web at *www.axis.com/techsup*

Set the Root Password

To access the Axis product, you must set the password for the default administrator user **root**. This is done in the **Configure Root Password** dialog, which opens when the product is accessed for the first time.

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See *HTTPS, on page 46*.

The default administrator user name **root** is permanent and cannot be deleted. If the password for root is lost, the product must be reset to the factory default settings. See *Reset to Factory Default Settings, on page 57*.

To set the password via a standard HTTP connection, enter it directly in the dialog.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click **Use HTTPS**.

   A temporary certificate (valid for one year) is created, enabling encryption of all traffic to and from the product, and the password can now be set securely.

2. Enter a password and then re-enter it to confirm the spelling.

3. Click **OK**. The password has now been configured.

Accessing the Product

The Live View Page

The controls and layout of the Live View page may have been customized to meet specific installation requirements and user preferences. Consequently, some of the examples and functions featured here may differ from those displayed in your own Live View page. The following provides an overview of each available control.

Controls on the Live View Page

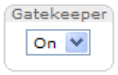
Select a stream profile for the Live View page from the **Stream Profile** drop-down list. For information about how to configure stream profiles, see *page 21*.

Click **Pulse** to activate the product's output port for a defined period of time. For information about how to enable and configure output buttons, see *page 27*.

Click the **Active/Inactive** buttons to manually activate and inactive the product's output port. For information about how to enable and configure output buttons, see *page 27*.

The **Manual Trigger** button is used to trigger an action rule from the Live View page. For information about how to configure and enable the button, see *Manual Trigger, on page 13*.

Click **Snapshot** to save a snapshot of the video image. Right-click the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AXIS Media Control viewer toolbar is not available. Enable this button from **Live View Config > Action Buttons.**



Enable or disable the **Gatekeeper** by selecting On or Off from the drop-down list. Read more about the Gatekeeper on *page 30*.

Manual Trigger

The **Manual Trigger** is used to trigger an action rule from the Live View page. The manual trigger can for example be used to validate actions during product installation and configuration.

To configure the manual trigger:

1. Go to **Setup > Events**.
2. Click **Add** to add a new action rule.
3. From the **Trigger** drop-down list, select **Input Signal**.
4. From the second drop-down list, select **Manual Trigger**.
5. Select the desired action and configure the other settings as required.

For more information about action rules, see *Events, on page 39*.

To show the manual trigger buttons in the Live View page:

1. Go to **Setup > Live View Config**.
2. Under **Action Buttons**, select **Show manual trigger button**.

Accessing the Product

AXIS Media Control viewer toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *AXIS Media Control (AMC), on page 16* for more information. The toolbar displays the following buttons:

The **Play** button connects to the Axis product and starts playing a media stream.

The **Stop** button stops the media stream.

The **Snapshot** button takes a snapshot of the video image. The location where the image is saved can be specified in the AMC Control Panel.

Click the **View Full Screen** button and the video image will fill the entire screen. Press ESC (Escape) on the computer keyboard to cancel full screen view.

The **Record** button is used to record the current video stream. The location where the recording is saved can be specified in the AMC Control Panel. Enable this button from **Live View Config** > **Viewer Settings.**

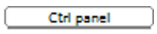
PTZ Controls

The Live View page also displays Pan/Tilt/Zoom (PTZ) controls. The administrator can enable/disable controls for specified users under **System Options > Security > Users**.

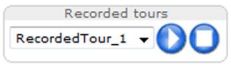
With the **PTZ Control Queue** enabled the time each user is in control of the PTZ settings is limited. Click the buttons to request or release control of the PTZ controls. The PTZ Control Queue is set up under **PTZ > Control Queue**.

Click the **Emulate joystick mode** button and click in the image to move the camera view in the direction of the mouse pointer.

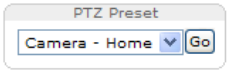
Click the **Center mode** button and click in the image to center the camera view on that position. The center mode button could also be used to zoom in on a specific area. Click in the image and drag to draw a rectangle surrounding the area to be magnified. To zoom out, rotate the mouse wheel.



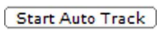
Click the **Ctrl panel** button to open the PTZ control panel which provides additional PTZ controls. User-defined buttons can also appear in the Control panel. See *Controls, on page 33*.



Select a recorded tour and click to play a previously recorded tour and click to stop. See *Tour Recording, on page 31*.

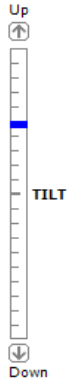


Select a PTZ preset position to steer the camera view to the saved position. See *Preset Positions, on page 29*.



Click the **Start Auto Track** button to start autotracking directly from the Live View page. See *Autotracking, on page 30*.

Accessing the Product



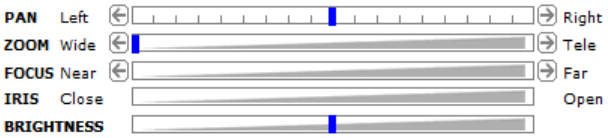
Pan and Tilt bars – Use the arrows to pan and tilt the camera view, or click on a position on the bar to steer the camera view to that position.

Zoom bar – Use the arrows to zoom in and out, or click on a position on the bar to zoom to that position.

Focus bar – Use the arrows to focus the camera, or click on a position on the bar to set the focus position. Using the focus bar will disable the product's autofocus. To re-enable, use the PTZ control panel which is opened by clicking the **Ctrl panel** button (see above).

Iris bar – Click on a position on the iris bar to change the degree to which the iris is opened. This will disable the product's auto iris. To re-enable, use the PTZ control panel which is opened by clicking the **Ctrl panel** button (see above).

Brightness bar – Click on a position on the brightness bar to adjust the image brightness. This setting will not be saved. To make a saved change, go to **Setup > Video > Camera Settings > Brightness** and adjust the brightness.



The PTZ controls can be disabled under **PTZ > Advanced > Controls**, see *Controls, on page 33*.

Media Streams

Media Streams

The Axis product provides several video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in the product provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can access video streams directly, without going via the Live View page.

How to Stream H.264

The video compression standard H.264 makes good use of bandwidth, and can provide high quality video streams at less than 1 Mbit/s.

Deciding which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. The available options in AXIS Media Control are:

Unicast RTP	This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to always have an up-to-date video stream, even if some images are dropped.	Unicasting is used for video-on-demand transmission so that there is no video traffic on the network until a client connects and requests the stream. Note that there are a maximum of 20 simultaneous unicast connections.
RTP over RTSP	This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.	
RTP over RTSP over HTTP	This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.	
Multicast RTP	This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some images are dropped. Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example. Note also that all multicast viewers count as one unicast viewer in the maximum total of 20 simultaneous connections.	

AXIS Media Control negotiates with the Axis product to determine the transport protocol to use. The order of priority, listed in the AMC Control Panel, can be changed and the options disabled, to suit specific requirements.

Note

H.264 is licensed technology. The Axis product includes one H.264 viewing client license. Installing additional unlicensed copies of the client is prohibited. To purchase additional licenses, contact your Axis reseller.

MJPEG

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the Axis product is to use the AXIS Media Control in Internet Explorer in Windows.

AXIS Media Control (AMC)

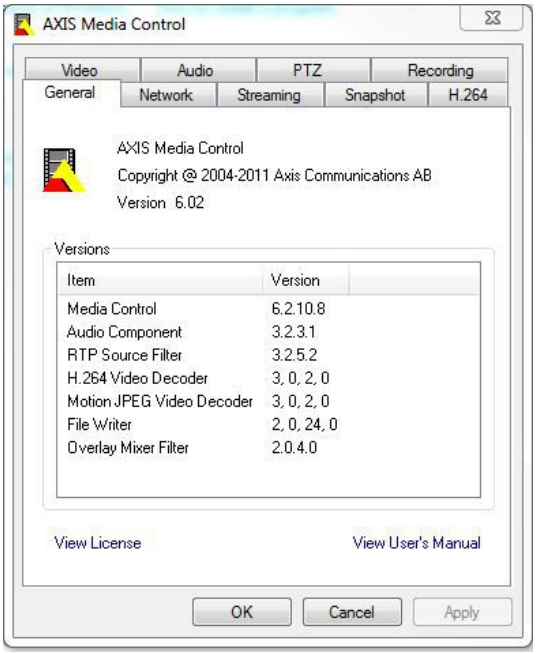
AXIS Media Control (AMC) in Internet Explorer in Windows is the recommended method of accessing live video from the Axis product.

Media Streams

The AMC Control Panel can be used to configure various video settings. Please see the AXIS Media Control User's Manual for more information.

The AMC Control Panel is automatically installed on first use, after which it can be configured. Open the AMC Control Panel from:

- Windows Control Panel (from the Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings**.



Alternative Methods of Accessing the Video Stream

You can also access video and images from the Axis product in the following ways:

- **Motion JPEG server push** (if supported by the client, Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- **Still JPEG images in a browser**. Enter the path `http://<ip>/axis-cgi/jpg/image.cgi`
- **Windows Media Player**. This requires AXIS Media Control and the H.264 decoder to be installed. The following paths can be used:
  - Unicast via RTP: `axrtpu://<ip>/axis-media/media.amp`
  - Unicast via RTSP: `axrtsp://<ip>/axis-media/media.amp`
  - Unicast via RTSP, tunneled via HTTP: `axrtsphttp://<ip>/axis-media/media.amp`
  - Multicast: `axrtpm://<ip>/axis-media/media.amp`
- **QuickTime™**. The following paths can be used:
  - `rtsp://<ip>/axis-media/media.amp`
  - `rtsp://<ip>/axis-media/media.3gp`

Media Streams

Note

- <ip>= IP addess
- The Axis product supports QuickTime 6.5.1 and later.
- QuickTime adds latency to the video stream.
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this.

Setting Up the Product

Setting Up the Product

The Axis product can be configured by users with administrator or operator rights. To open the product's Setup pages, click **Setup** in the top right-hand corner of the Live View page.

- **Administrators** have unrestricted access to all settings.
- **Operators** have access to all settings except System Options

See also the online help .

Basic Setup

Basic Setup provides shortcuts to the settings that should be made before using the Axis product:

1. Users. See *page 46*.
2. TCP/IP. See *page 48*.
3. Date & Time. See *page 48*.
4. Video Stream. See *page 20*.

The Basic Setup menu can be disabled from **System Options > Security > Users**.

Video

Video

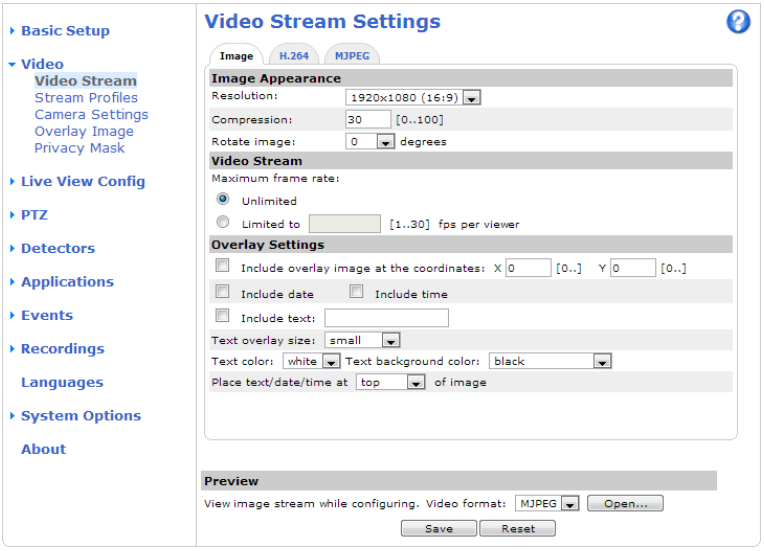
It is possible to configure the following video features in your Axis product:

- Video stream. See *page 20*.
- Stream profiles. See *page 21*.
- Camera settings. See *page 22*.
- Overlay image. See *page 23*.
- Privacy mask. See *page 24*.

Video Stream

You can define the following video stream settings from **Video** > **Video Stream**:

- Image. See *page 21*.
- H.264. See *page 21*.
- MJPEG. See *page 21*.



Pixel Counter

The pixel counter shows the number of pixels in an area of the image. The pixel counter is useful in situations where there is a requirement that the image is a certain size, for example in face recognition.

The pixel counter can be accessed from:

- **Video** > **Video Stream**. Under **Preview**, click **Open** and select the **Show pixel counter** option to enable the rectangle in the image. Use the mouse to move and resize the rectangle, or enter the number of pixels in the **Width** and **Height** fields and click **Apply**.
- The Live View page in Internet Explorer in Windows. Right-click in the image and select **Pixel counter**. Use the mouse to move and resize the rectangle.

Video

Image

The default image settings can be configured under **Video> Video Stream**. Select the **Image** tab.

The following settings are available:

- **Resolution**. Select the default resolution.
- **Compression**. The compression level affects the image quality, bandwidth and file size of saved images; the lower the compression, the higher the image quality with higher bandwidth requirements and larger file sizes.
- **Rotate image**. If required, the image can be rotated.
- **Maximum frame rate**. To avoid bandwidth problems, the frame rate allowed to each viewer can be **Limited to** a fixed amount. Alternatively, the frame rate can be set as **Unlimited**, which means the Axis product always delivers the highest frame rate possible under the current conditions.
- **Overlay settings**. See *Overlay, on page 23*.

Click **Save** to apply the new settings.

H.264

H.264, also known as MPEG-4 Part 10/AVC, is a video compression standard that provides high quality video streams at low bit rates. An H.264 video stream consists of different types of frames such as I-frames and P-frames. An I-frame is a complete image whereas P-frames only contain the differences from previous frames.

The **GOV length** is the number of frames between two consecutive I-frames. Increasing the GOV length may save considerably on bandwidth requirements in some cases, but may also have an adverse affect on image quality.

The Axis product supports two **H.264 profiles**. The Main profile provides higher compression than the Baseline profile with the same video quality, but requires more processing power to decode.

The bit rate can be set as **Variable Bit Rate** (VBR) or **Constant Bit Rate** (CBR). VBR adjusts the bit rate according to the image complexity, using up more bandwidth for increased activity in the image, and less for lower image activity. CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either frame rate or image quality. Not setting a priority means that frame rate and image quality are equally affected. You must save your settings before they can take effect.

The current bit rate can be set to appear as text overlay. To do this, select the **Include text** check box option under **Overlay Settings** and enter the modifier `#b` in the field.

MJPEG

Sometimes the image size is large due to low light or complex scenery. Adjusting the maximum frame size helps to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Setting the frame size to the **Default** setting provides consistently good image quality at the expense of increased bandwidth and storage usage in low light. Limiting the frame size optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the maximum frame size should be set to an optimal value.

Stream Profiles

A stream profile is a set of predefined stream settings including resolution, compression, frame rate and overlay settings. Stream profiles can be used:

- When setting up recording using action rules. See *Events, on page 39*.
- When setting up continuous recording. See *Continuous Recording, on page 44*.
- In the Live View page – select the stream profile from the **Stream profile** drop-down list.

Video

For quick setup, use one of the predefined stream profiles. Each predefined profile has a descriptive name, indicating its purpose. If required, the predefined stream profiles can be modified and new customized stream profiles can be created.

To create a new profile or modify an existing profile, go to **Setup > Video** > **Stream Profiles**.

To select a default stream profile for the Live View page, go to **Setup > Live View Config**.

Camera Settings

The **Video > Camera Settings** page provides access to advanced image settings for the Axis product.

Image Appearance

Increasing the **Color level** increases the color saturation. The value 100 gives maximum color saturation. The value 0 gives a black and white image.

The image **Brightness** can be adjusted in the range 0–100, where a higher value produces a brighter image.

Increasing the **Sharpness** can increase bandwidth usage. A sharper image might increase image noise especially in low light conditions. A lower setting reduces image noise, but the whole image will appear less sharp.

White Balance

White balance is used to make colors in the image appear the same regardless of the color temperature of the light source. The Axis product can be set to automatically identify the light source and compensate for its color. Alternatively, select the type of light source from the drop-down list. For a description of each available setting, see the online help.

Wide Dynamic Range

Wide dynamic range can improve the exposure when there is a considerable contrast between light and dark areas in the image. Enable WDR in intense backlight conditions. The different WDR settings adjust for various amounts of contrast in the image. Use a higher WDR number for a higher contrast. Disable WDR in low light conditions for optimal exposure.

Exposure Settings

Exposure control – These settings is used to adapt to the amount of light used. **Automatic** is the default setting and it can be used in most situations. The shutter speed is automatically set to produce optimum image quality. Use **Manual** if you have special requirements for the exposure setting and wish to lock it. Select the desired exposure time from the drop-down list.

Max exposure time – Select the maximum exposure time from the drop-down list. Increasing the exposure time will improve image quality, but decrease the frame rate. There may also be an increase in motion blur. Checking **Allow slow shutter** decreases the shutter speed in low light to improve image brightness.

Enable Backlight compensation – Select Enable Backlight compensation if a bright spot of light, for example a light bulb, causes other areas in the image to appear too dark.

Highlight Compensation – The Axis product will detect a bright light from a source such as a torch or car headlights and mask that image area. This setting is useful when the camera operates in a very dark area where a bright light may overexpose part of the image and prevent the operator from seeing other parts of the scene.

Max gain – Measured in decibels (dB), gain describes the amount of amplification applied to a signal, in this case the visual information in the image. A high level of amplification may provide a better image in very low light situations. A high gain will also increase the amount of image noise.

Exposure zones – This settings determines which part of the image is used to calculate the exposure. For most situations, the **Auto** setting can be used. For particular requirement, select a predefined area.

IR cut filter – The IR cut filter prevents infrared (IR) light from reaching the image sensor. In poor lighting conditions, for example at night, or when using an external IR lamp, set the IR cut filter to **Off**. This increases light sensitivity and allows the product to "see"

infrared light. The image is shown in black and white when the IR cut filter is off. Set the IR cut filter to **Auto** to automatically switch between **On** and **Off** according to the lighting conditions.

Day/Night shift priority – Use the **Day/Night shift priority** bar to determine when the camera shifts into either day mode or night mode. By default, the camera will automatically change from day to night mode at a pre-defined level which corresponds to light conditions. By dragging the bar handle towards the sun, the camera will change to day mode earlier and change to night mode late.

Image Settings

Autofocus enabled – Automatic focusing is enabled by default. If the focus position is changed manually using the focus bar, autofocus will be disabled even if enabled here. In this case, use the PTZ control panel to enable autofocus, see *PTZ Controls, on page 14*. If required, the focus control can be disabled under **PTZ > Advanced > Controls**.

Noise reduction – Set to **On** to enable noise reduction. Noise reduction may increase the amount of motion blur.

Image freeze on PTZ – Select **All movements** to freeze the image while the camera is moving during a pan, tilt or zoom operation. Once the camera reaches its new position, the view from that position is shown. **Presets** freezes the image only when the camera moves between preset positions.

Overlay

Overlays are used to provide extra information, for example for forensic video analysis or during product installation and configuration. Overlays are superimposed over the video stream.

An overlay text can display the current date and time, or a text string. When using a text string, modifiers can be used to display information such as the current bit rate or the current frame rate. For information about available modifiers, see *File Naming & Date/Time Formats* in the online help .

It is also possible to display text when an action rule is triggered, see *Using Overlay Text in an Action Rule*.

To enable overlays:

1. Go to **Video > Video Stream** and select the **Image** tab.
2. To include an overlay image, select **Include overlay image at the coordinates**. The overlay image must first be uploaded to the Axis product, see *Overlay Image*.
3. To include date and time, select **Include date** and **Include time**.
4. To include a text string, select **Include text** and enter the text in the field. Modifiers can be used, see *File Naming & Date/Time Formats* in the online help .
5. Define text overlay characteristics in the relevant fields.
6. Click **Save**.

To modify the date and time format, go to **System Options > Date & Time**. See *Date & Time, on page 48*.

Overlay Image

An overlay image is a static image superimposed over the video stream. The image, for example company logo, is used to provide extra information or to mask a part of the image.

Since it is static, the position and size of an overlay image will remain the same regardless of resolution and Pan/Tilt/Zoom movements. To set up a dynamic mask, which will always mask the specified part of monitored area, see *Privacy Mask*.

To use an overlay image, the image must first be uploaded to the Axis product:

1. Go to **Video** > **Overlay Image**.
2. Click **Browse** and browse to the file.

3. Click **Upload**.
4. Select the image to use from the **Use overlay image** list.
5. Click **Save**.

To display the overlay image:

1. Go to **Video** > **Video Stream** and select the **Image** tab.
2. Under **Overlay Settings**, select **Include overlay image at the coordinates** and enter the X and Y coordinates.
3. Click **Save**.

For information about supported image formats, see the online help .

Using Overlay Text in an Action Rule

Action rules, see *page 39*, can display an overlay text when the rule is triggered. The text can be used to provide information for forensic video analysis, notify surveillance operators or validate triggers and actions during product installation and configuration.

To display overlay text when an action rule is triggered, the modifier `#D` should be used as described below. When the rule is triggered, `#D` will be replaced by the text specified in the action rule.

Start by enabling overlay text in the video stream:

1. Go to **Video > Video Stream** and select the **Image** tab.
2. Under **Overlay Settings**, select **Include text**.
3. Enter the modifier `#D` and, optionally, additional text which will be displayed also when the action rule is not active.

Create the action rule:

1. Go to **Events > Action Rules**
2. Click **Add** to create a new rule.
3. Select a **Trigger** and, optionally, a **Schedule** and **Additional conditions**. See the online help for details.
4. From the **Actions** list, select **Overlay Text**
5. Enter the text to display in the **Text** field. This is the text that `#D` will be replaced by.
6. Specify the **Duration**. The text can be displayed while the rule is active or for a fixed number of seconds.

Example

To display the text "Motion detected" when motion is detected, enter `#D` in the **Include text** field and enter "Motion detected" in the **Text** field when setting up the action rule.

Privacy Mask

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. Privacy masks cannot be bypassed via the VAPIX® Application Programming Interface (API).

The Privacy Mask List, **Video** > **Privacy Mask**, shows all the masks that are currently configured in the Axis product and indicates if they are enabled.

Since the Pan/Tilt/Zoom coordinates define its size and position, a privacy mask is dynamic in relation to the monitored area. This means that regardless of the angle and zoom of the lens, the same place or object will be hidden. To define at what magnification the mask should be displayed, zoom to the desired level and click **Set level**.

You can add a new mask, re-size the mask with the mouse, choose a color for the mask, and give the mask a name.

Video

For more information, see the online help .

Important

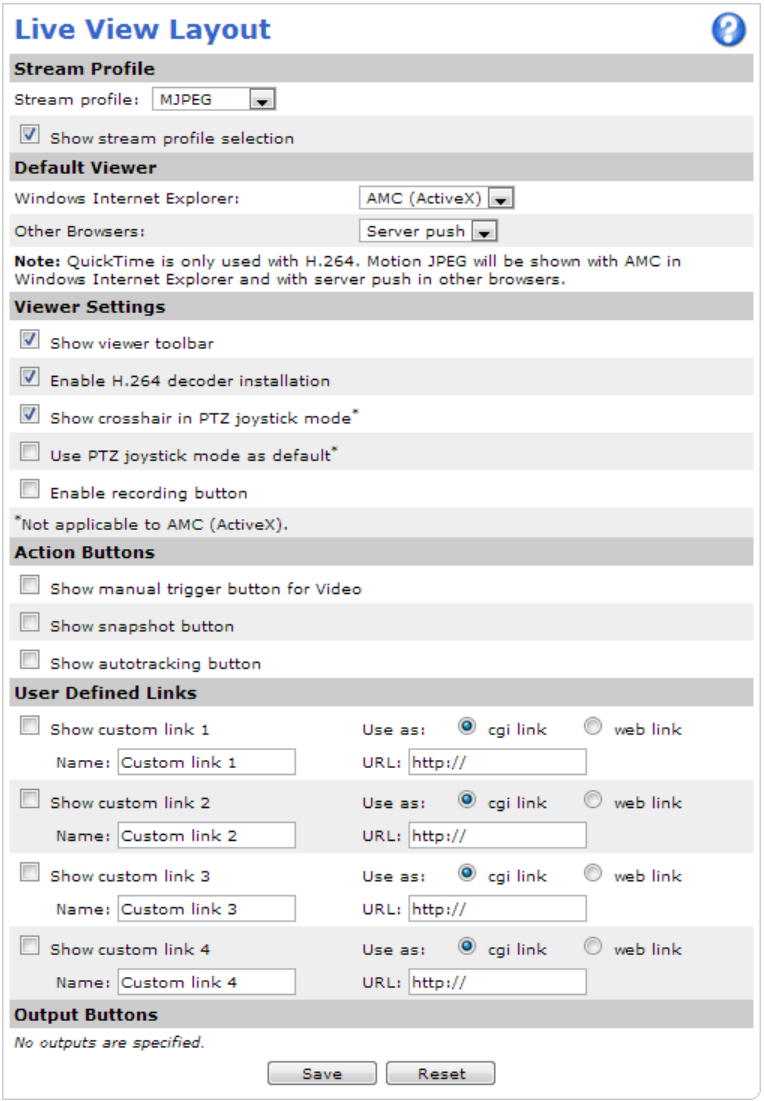
Adding many privacy masks may affect the product's performance.

Live View Config

Live View Config

You can customize the Live View page and alter it to suit your requirements. It is possible to define the following features of the Live View page.

- Stream Profile. See *page 21*.
- Default Viewer for Browser. See *page 27*.
- Viewer Settings. See *page 27*.
- Action Buttons. These are the buttons described in *Controls on the Live View Page, on page 13*.
- User Defined Links. See *page 27*.
- Output Buttons. See *page 27*.



Live View Config

Default Viewer for Browsers

From **Live View Config** > **Default Viewer** select the default method for viewing video images in your browser. The product attempts to show the video images in the selected video format and viewer. If this is not possible, the product overrides the settings and selects the best available combination.

Browser	Viewer	Description
Windows Internet Explorer	AMC	Recommended viewer in Internet Explorer (H.264/Motion JPEG).
	QuickTime	H.264.
	Java applet	A slower imaging alternative to AMC (Motion JPEG). Requires one of the following installed on the client: • JVM (J2SE) 1.4.2 or higher. • JRE (J2SE) 5.0 or higher.
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.
Other browsers	Server Push	Recommended viewer for other browsers (Motion JPEG).
	QuickTime	H.264.
	Java applet	A slower imaging alternative to Server Push (Motion JPEG only).
	Still image	Displays still images only. Click the Refresh button in your browser to view a new image.

For more information, please see the online help .

Viewer Settings

To configure options for the viewer, go to **Live View Config > Viewer Settings**.

- Select **Show viewer toolbar** to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.
- **H.264 decoder installation**. The administrator can disable installation of the H.264 decoder included with AXIS Media Control. This is used to prevent installation of unlicensed copies. Further decoder licenses can be purchased from your Axis reseller.
- Select **Show crosshair in PTZ joystick mode** to enable a cross that will indicate the center of the image in PTZ joystick mode.
- Select **Use PTZ joystick mode as default** to enable joystick mode. The mode can be changed temporarily from the PTZ control panel.
- Select **Enable recording button** to enable recording from the Live View page. This button is available when using the AMC viewer. The recordings are saved to the location specified in the AMC Control Panel. See *AXIS Media Control (AMC), on page 16*.

User Defined Links

To display user-defined links in the Live View page, select the **Show custom link** option, give the link a name and then enter the URL to link to. When defining a web link do not remove the 'http://' from the URL address. Custom links can be used to run scripts or activate external devices connected to the product, or they can link to a web page. Custom links defined as cgi links will run the script in the background, in a hidden frame. Defining the link as a web link will open the link in a new window.

Output Buttons

External I/O devices connected to the Axis product's output ports can be controlled directly from the Live View page.

Live View Config

Note

To enable this setting at least one I/O port must be configured as an output port. See *I/O Ports, on page 55*.

To display output buttons in the Live View page:

1. Go to **Setup > Live View Config**.
2. Under **Output Buttons**, select the type of control to use:
   - **Pulse** activates the output for a defined period of time. The pulse time can be set from 1/100 second to 60 seconds.
   - **Active/Inactive** displays two buttons, one or each action.

To configure the active and inactive states, go to **System Options > Ports & Devices > I/O Ports** and set the port's **Normal state**.

For more information about I/O ports, see *I/O Ports, on page 55*.

PTZ (Pan Tilt Zoom)

Preset Positions

A preset position is a predefined view that can be used to quickly steer the camera to a specific location. Preset positions can be accessed in several ways:

- By selecting the preset from the **Preset positions** drop-down list in the Live View Page.
- When setting up action rules. See *page 39*.
- When setting up Guard Tour. See *page 31*.
- When setting up the Gatekeeper. See *page 30*

To add a preset position:

1. Go to **PTZ > Preset Positions**.
2. Use the pan, tilt and zoom controls to steer the camera view to the desired position.
3. Enter a descriptive name in the **Current position** field.
4. If required, select **Use current position as Home**.
5. Click **Add**. The camera's position, iris and focus settings are saved as a preset position.

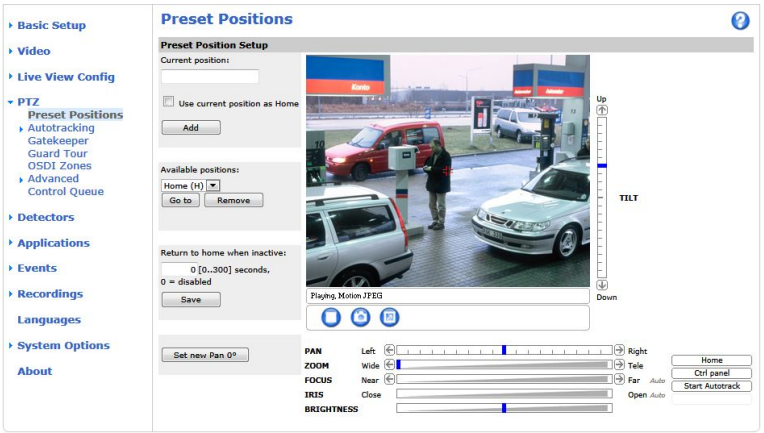
The **Home** position is readily accessible by clicking the **Home** button on the Live View page and in the Preset Positions setup window.

To set a customized home position, select **Use current position as Home** when adding a preset position. The user-defined home position will have (H) added, for example, Entrance (H). The default Home position, called "Home", will still be available.

The product can be configured to return to the Home position when the PTZ functionality has been inactive for a specified length of time. Enter the length of time in the **Return to home when inactive** field and click **Save**. Set the time to zero to prevent the product from automatically returning to the Home position.

To include the preset position name in the overlay text, go to **Video**, select **Include overlay text** and enter the modifier `#P` in the field. For more information about modifiers, see *File Naming & Date/Time Formats* in the online help .

The product can be mounted in three different horizontal directions. This may cause the view from Pan 0° to be changed from the original view. Click **Set new Pan 0°** to set the pan coordinate system to zero in the current direction. Set new Pan 0° can be useful for instance when re-installing the product after maintenance. Note that, setting Pan 0° will affect all previously defined presets, guard tours, masks etc.



PTZ (Pan Tilt Zoom)

Gatekeeper

The Active Gatekeeper monitors an area such as an entrance gate. When motion is detected in the monitored area, the Gatekeeper will, depending on configuration, steer the camera to a selected preset position or start autotracking from a selected preset position. Using a zoomed-in preset position can make it possible to, for example, read a license plate or identify a person. When motion is no longer detected, the camera returns to its Home position after a defined time.

To enable the Gatekeeper, go to **PTZ > Gatekeeper** and follow the online instructions.

It is also possible to, for example, record video or save images (take a snapshot) while the Gatekeeper is active. Go to **Events** and set up an action rule with **PTZ Preset Reached** or **Autotracking** as trigger.

Autotracking

The Axis product can detect movement in the field of view, for example a moving vehicle or person. If autotracking is enabled, the Axis product will automatically pan and tilt to follow the moving object. In case there is much simultaneous movement, the area with the most movement will be followed. Autotracking continues until the moving object stops or disappears from the monitored area. Movement in areas blocked by privacy masks and in exclude areas does not trigger autotracking.

It is strongly recommended to enable the PTZ **Control Queue** if autotracking and guard tour are enabled simultaneously. In the PTZ Control Queue, guard tour has lower priority than autotracking, so autotracking will not be abandoned to start a guard tour.

Configuration

Start/Stop Autotracking – Click **Start** to enable autotracking. To disable autotracking, click **Stop**.

Settings – The Movement trigger sensitivity level can be set to **Low**, **Medium** or **High**. Medium is usually a good choice, depending on the size of the moving objects and the image contrast, a low or high sensitivity might be more suitable.

Exclude Areas

Exclude areas are areas where movement is to be ignored.

Note

Movement in an area blocked by a privacy mask is always ignored.

1. Click **Add area** to create an exclude area
2. Resize and move the area (the blue rectangle) to the desired position.
3. Enter a descriptive name and click **Save**.

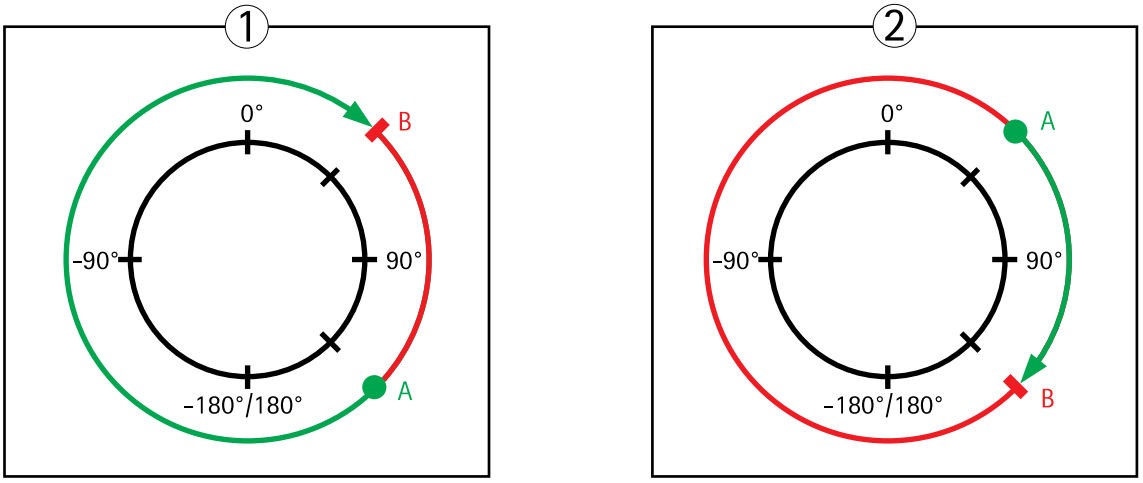
To remove an area, click the name of the area and click **Remove**. To enable or disable an area, click the name of the area and click **Enable/Disable**.

Max Limits

The pan and tilt limits restrict the area where autotracking is allowed. The area beyond the set limits will be ignored. This may prove useful, for example, to avoid tracking birds in the sky. Between the pan start and end limits, autotracking is allowed going clockwise. The illustrations show the difference between setting a range from 135° to 45° (1) and a range from 45° to 135° (2).

1. Select **Enable tilt limit** and **Enable pan limit** respectively to enable the tilt and pan limits.
2. Enter the Tilt angle and Pan limit values, or click the links and move the blue horizontal and vertical bars in the preview window until satisfied.
3. Click **Save**.

PTZ (Pan Tilt Zoom)



Top view

A Pan limit start
B Pan limit end

Guard Tour

A guard tour displays the video stream from different preset positions, one-by-one, in a predetermined order or at random and for configurable time periods. The enabled guard tour will keep running after the user has logged off or closed the browser.

The guard tour capability in this Axis product also includes tour recording. Tour recording is described in *Tour Recording, on page 31*.

To add a guard tour:

1. Go to **PTZ > Guard Tour** and click **Add**.
2. Select **Create a preset tour** and click **OK**.
3. Enter a descriptive name.
4. Specify the pause length between runs.
5. Select an available preset position and click **Apply**.
6. Specify the **Move Speed**.
7. Specify the **View Time** in seconds or minutes.
8. Specify the **View Order** or select the **Random view order** option.
9. Click **Save**.

To modify or remove guard tours, go to **PTZ > Guard Tour**, select the guard tour in the **Guard Tour List** and click **Modify/Remove**.

For more information see the online help .

Tour Recording

The guard tour function in this product includes tour recording, which allows recording of a custom tour using an input device such as a joystick, mouse, keyboard or through the VAPIX® Application Programming Interface (API). A recorded tour displays the video stream of the recorded sequence of Pan/Tilt/Zoom movements, including their variable speeds and lengths.

To add a recorded tour:

1. Go to **PTZ > Guard Tour** and click **Add**.
2. Select **Create a record tour** and click **OK**.
3. Enter a descriptive name.
4. Specify the pause length between runs.
5. Click to start recording the Pan/Tilt/Zoom movements.
6. When satisfied, click .
7. Click **OK**.

Note

Only the name of the recorded tour and pause between runs can be modified. Starting a new recording will overwrite the existing guard tour.

The recorded tour can be activated from the Live View and Guard Tour pages or through events. For more information see the online help .

OSDI Zones

On-Screen Direction Indicator (OSDI) zones can be included in the overlay text (see *Overlay, on page 23*) to aid the user to navigate the Axis product. Each OSDI zone is set up with coordinates and a descriptive name.

OSDI zones are set up under **PTZ > OSDI Zones**. The Axis product uses the coordinates of the center of the view to set the lower left and upper right zone areas. First navigate to where you would like the lowermost left point of the OSDI zone to be located. Click **Get** to set the coordinates. Proceed to where the upper right point of zone should be located and click **Get**. Give the zone a descriptive name and click **OK**.

To include the name of the OSDI zone in the overlay text, go to **Video < Video Stream < Overlay Settings**. Check the **Include text** box and enter the modifier `#L` in the field. For more information about modifiers, see *File Naming & Date/Time Formats* in the online help .

Advanced

Limits

Define the pan, tilt, zoom and focus limits for the Axis product. Movements to the left and right, up and down, can be restricted to narrow the area under surveillance.

Configure the near focus limit to avoid focusing on objects too close to the camera lens.

When **Enable E-flip** is selected, as it tilts down and continues to pan backwards, the Axis product will automatically correct the view and flip it 180 degrees. The left limit must be set to –180 degrees and the right limit to 180 degrees for e-flip to work.

Move speed sets the speed of the camera's pan and tilt movements. The default setting is maximum speed.

When using a joystick (or emulating one with the mouse) the **Enable proportional speed** setting can be used to reduce the maximum pan/tilt movement speed, i.e. the speed the camera view moves at when the joystick is pushed all the way out in any direction. This is useful then the view is zoomed in on an object.

See the online help for more information.

PTZ (Pan Tilt Zoom)

Controls

Panel Shortcut Command Buttons can be configured to provide direct access to commands issued via the VAPIX® Application Programming Interface. The buttons will be displayed in the PTZ control panel, which is available in the Live View page through the **Ctrl panel** button, see *page 14*.

Deselect the options under **Enable/Disable controls** to disable the pan, tilt, zoom, focus and iris controls.

Note

Disabling PTZ controls will not affect preset positions. For example, if the tilt control is disabled, the product can still move to preset positions that require a tilt movement.

Control Queue

The administrator can set up a queue for PTZ controllers from **PTZ > Control Queue**. Once set up, the **PTZ Control Queue** buttons appear in the Live View page offering one viewer exclusive control for a limited period of time. Other users will be placed in queue.

A user who belongs to a group (see *Users, on page 46*) with a higher PTZ priority can go before other users in the queue and take control of the product. The order of priority is as follows:

1. **Administrator** – An administrator takes over PTZ control regardless of who is first in queue. The administrator will be removed from the queue 60 seconds after the last PTZ control command.
2. **Event** – The Axis product can be configured to go to a preset position when triggered by an alarm (see *Events, on page 39*). The event will immediately be placed first in the queue except when an administrator is in control.
3. **Operator** – Same as administrator but with lower priority
4. **Guard Tour** – A guard tour (see *page 31*) has PTZ control for an indefinite period of time. It may be overridden by an operator, event or administrator. The guard tour will resume when higher priority groups leave the queue.
5. **Viewer** – Multiple viewers must wait for their turn. The viewer has 60 seconds PTZ control before control is passed on to the next viewer in queue.

Note

- The administrator can enable and disable PTZ controls for selected users.
- To identify different users in the viewer group, cookies must be enabled on the client.

Detectors

Detectors

Shock Detection

Enable **Shock Detection** from the **Detectors** menu. Shock detection is used, for example, to generate an alarm if the product is hit by an object.

Use the **Shock sensitivity** slider to adjust the sensitivity level at which the product should send an alarm upon being hit. Low sensitivity value implies that the product will generate an alarm only if the hit is powerful.

Motion Detection

Motion detection is used to generate an alarm whenever movement starts or stops in the camera view.

Motion detection is configured by defining up to 10 Include and Exclude windows:

- **Include windows** – define areas where motion should be detected
- **Exclude windows** – define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored).

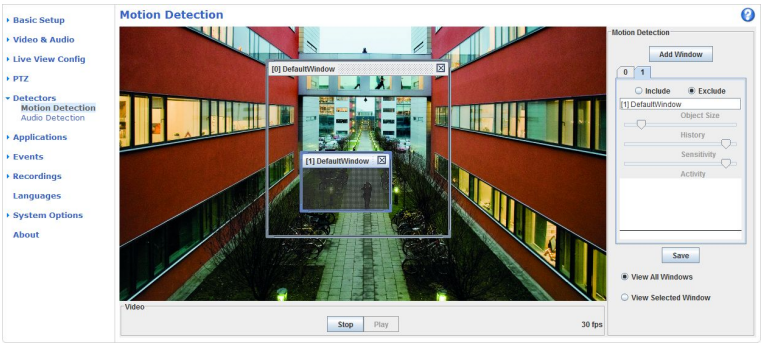
For instructions, see *Set Up Motion Detection Windows, on page 34*.

To control the number of motion detection alarms, the parameters **Object Size**, **History** and **Sensitivity** can be adjusted. See *Motion Detection Parameters, on page 35*.

Once motion detection windows are configured, the Axis product can be configured to perform actions when motion is detected. Possible actions include uploading images and start recording. For more information, see *Setting Up an Action Rule, on page 40*.

Note

- Using the motion detection feature may decrease the product's overall performance.
- The position of the Motion Detection Window is relative to the orientation of the Camera. Changing the orientation of the camera will also change the position of the Motion Detection Window.



Set Up Motion Detection Windows

To set up a motion detection Include Window, follow these instructions:

1. Go to **Detectors > Motion Detection**.
2. Select the **Configure Included Windows** option and click **New**. Select the new window in the list of windows and enter a descriptive name.
3. Adjust the size (drag the bottom right-hand corner) and the position (click on the text at the top and drag to the desired position) of the window.

Detectors

4. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see *Motion Detection Parameters* for details). Any detected motion within an active window is indicated by red peaks in the **Activity window**.
5. Click **Save**.

To exclude parts of the include window, select the **Configure Excluded Windows** and position the exclude window within the include window.

To delete an include or exclude window, select the window in the list of windows and click **Del**.

Motion Detection Parameters

The parameters controlling motion detection are described in the table below:

Parameter	Object Size	History	Sensitivity
Description	Object size relative to window size.	Object memory length.	Difference in luminance between background and object.
High level (100%)	Only very large objects trigger motion detection.	An object that appears in the window triggers motion detection for a long time before it is considered as non-moving.	Ordinary colored objects on ordinary backgrounds trigger motion detection.
Medium level (50%)			A large difference in luminance is required to trigger motion detection.
Low level (0%)	Even very small objects trigger motion detection.	An object that appears in the window triggers motion detection only for a very short time before it is considered as non-moving.	Only very bright objects on a dark background trigger motion detection.
Recommended values	5–15%	60–90%	75–95%
Default values	15%	90%	90%

Note

- To trigger on small objects or movements, use several small motion detection windows rather than one large window and select a low object size.
- To avoid triggering on small objects, select a high object size.
- While monitoring an area where moving objects are not expected, select a high history level. This will cause motion detection to trigger as long as the object is present in the window.
- To only detect flashing light, select a low sensitivity. In other cases high sensitivity is recommended.

Object Removed

Object Removed is used to trigger an alarm if an object, within a pre-defined area of interest, is removed. Object Removed provides tools to define:

Area of interest – This is a virtual area that is defined around an object to detect if that object has been removed from the scene.

Object size – Defines the size of the objects that should be detected.

Sensitivity – Use this slidebar to define how sensitive the detection should be.

Drawing Opacity – Use this slidebar to define how transparent the area of interest shape should be. Note that, this change will not be saved.

Detectors

See the online help for more information.

Enter/Exit Detector

Enter/Exit Detector is used to trigger an alarm if an object, within a pre-defined area of interest, has entered or left the area. Enter/Exit Detector provides tools to define:

Area of interest – This is a virtual area that is defined to detect moving objects entering a defined area

Object size – Defines the size of the objects that should be detected.

Sensitivity – Use this slidebar to define how sensitive the detection should be.

Drawing Opacity – Use this slidebar to define how transparent the area of interest shape should be. Note that, this change will not be saved.

See the online help for more information.

Fence Detector

Fence Detector is used to trigger an alarm if an object crosses a virtual line. Fence Detector provides tools to define:

Area of interest – This is a virtual line that is defined to detect objects moving across it.

Object size – Defines the size of the objects that should be detected.

Sensitivity – Use this slidebar to define how sensitive the detection should be.

Drawing Opacity – Use this slidebar to define how transparent the area of interest shape should be. Note that, this change will not be saved.

See the online help for more information.

Object Counter

Object Counter is used to count objects that move across a virtual line. Object Counter provides tools to define:

Area of interest – This is a virtual line that is defined to detect objects moving across it keep count.

Object size – Defines the size of the objects that should be detected.

Sensitivity – Use this slidebar to define how sensitive the detection should be.

Drawing Opacity – Use this slidebar to define how transparent the area of interest shape should be. Note that, this change will not be saved.

See the online help for more information.

Applications

Applications

Third party applications can be uploaded to and installed on the Axis product. Applications add functionality to the product, for example video analytics and intelligent video capabilities such as recognition, tracking, detection and counting. For information about available applications, downloads, trials and licenses, go to *www.axis.com/applications*

Note

- It is recommended to run one application at a time.
- Avoid running applications when the built-in motion detection is active.

Application Licenses

Some applications need a license to run. Licenses can be installed in two ways:

- Automatic installation — requires access to the Internet
- Manual installation — obtain the license key from the application vendor and upload the key to the Axis product

To request a license, the Axis product serial number (S/N) is required. The serial number can be found on the product label and under **System Options > Support > System Overview**.

Install Application

To install and start an application:

1. Go to **Setup > Applications**.
2. Under **Upload Application**, click **Browse**. Locate the application file and click **Upload Package**.
3. Install the license (if applicable). For instructions, see the documentation provided by the application vendor.
4. Start the application. Go to page **Applications**, select the application in the list of installed applications and click **Start**.
5. Configure the application. For instructions, see the documentation provided by the application vendor.

Note

- Applications can be uploaded by product administrators.
- Applications and licenses can be installed on multiple products at the same time using AXIS Camera Management, version 3.10 and later.

To generate a log file for the application, go to **Applications**. Select the application and click **Log**.

Application Considerations

If an application is upgraded, application settings, including the license, will be removed. The license must be reinstalled and the application reconfigured.

If the Axis product's firmware is upgraded, installed applications and their settings will remain unchanged, although this is not guaranteed by Axis Communications AB. Note that the application must be supported by the new firmware. For information about firmware upgrades, see *Upgrading the Firmware*.

If the Axis product is restarted, running applications will restart automatically.

If the Axis product is restored, installed applications remain unchanged but must be restarted. To start the application, go to **Setup > Applications**. Select the application in the list of installed applications and click **Start**. For information about restoring the Axis product, see *Maintenance*.

Applications

If the Axis product is reset to factory default, installed applications and their settings are removed. For information about factory default, see *Reset to Factory Default Settings*.

Events

Events

The Axis product can be configured to perform actions when different events occur, for example, start a recording when motion is detected. The set of conditions that defines how and when the action is triggered is called an **Action Rule**.

Available action rule **triggers** and **conditions** include:

- **Applications** – Use installed applications to trigger the rule. See *Applications, on page 37*.
- **Detectors**
  - **Live Stream Accessed** – Trigger the rule when any stream is accessed and during edge storage playback. This can for example be used to send notifications.
  - **Motion Detection** – Trigger the rule when motion is detected. See *Motion Detection, on page 34*.
  - **Shock Detected** – Trigger the rule when the Axis product detects it has been tilted or hit. See *Shock Detection, on page 34*.
  - **Enter/Exit** – Trigger the rule when an object has entered or exited the area. See *Enter/Exit Detector, on page 36*.
  - **Fence Detector** – Trigger the rule when an object has crossed a virtual line. See *Fence Detector, on page 36*
  - **Object Removed** – Trigger the rule when an object has been removed from a scene. See *Object Removed, on page 35*.
- **Hardware**
  - **Heater** – Trigger the rule if the heater is malfunctioning. This can for example be used to send maintenance notifications.
  - **Network** – Trigger the rule if network connection is lost or restored. This can for example be used to start recording to the SD card.
  - **Temperature** – Trigger the rule if the temperature falls outside or inside the operating range of the product. This can for example be used to send maintenance notifications.
- **Input Signal**
  - **Digital Input Port** – Trigger the rule when an I/O port receives a signal from a connected device. See *I/O Ports, on page 55*.
  - **Manual Trigger** – Trigger the rule using the **Manual Trigger** button in the Live View page. See *Controls on the Live View Page, on page 13*. This can for example be used to validate actions during product installation and configuration.
  - **Virtual Inputs** – can be used by a VMS (Video Management System) to trigger actions. Virtual inputs can, for example, be connected to buttons in the VMS user interface.
- **PTZ**
  - **Autotracking** – Trigger the rule when autotracking starts or stops. See *Autotracking, on page 30*.
  - **Error** – Trigger the rule if the PTZ functionality is not working correctly. This can for example be used to send maintenance notifications.
  - **Moving** – Trigger the rule when the camera view moves due to a PTZ operation. This can for example be used as an additional condition to prevent an action rule triggered by motion detection to record video while the camera view moves due to a PTZ operation.
  - **Preset Reached** – Trigger the rule when the camera stops at a preset position. This can be for example be used with the Send Images action to upload images from the preset position.

- **Ready** – Trigger the rule when the PTZ functionality is ready to be used. This can for example be used to steer the camera to a specific preset position when the product is started.

- **Storage**
  - **Disruption** – Trigger the rule if storage problems are detected, for example if the storage device is unavailable, removed, full, locked or if other read or write problems occur. This can for example be used to send maintenance notifications.
  - **Recording** – Triggers the rule when the Axis product records to the storage device. The recording status trigger can be used to notify the operator, for example by flashing LED lights, if the product has started or stopped to record to the storage device. Note that, this trigger can be used only for edge storage recording status.

- **System**
  - **System Ready** – Trigger the rule when the product has been started and all services are running. This can for example be used to send a notification when the product restarts.

- **Time**
  - **Recurrence** – Trigger the rule periodically. See *Recurrences, on page 43*. This can for example be used to upload an image every 5 minutes.
  - **Use Schedule** – Trigger the rule according to the selected schedule. See *Schedules, on page 42*.

Available **actions** include:

- **Day/Night Vision Mode** – Set day mode (IR cut filter on) or night mode (IR cut filter off).
- **Output Port** – Activate an I/O port to control an external device.
- **Overlay Text** – Display an overlay text. See *Using Overlay Text in an Action Rule, on page 24*.
- **PTZ Control**
  - **Autotracking** – Start autotracking. See *Autotracking, on page 30*.
  - **Preset Position** – Go to a preset position.
  - **Guard Tour** – Start a guard tour. See *Guard Tour, on page 31*.
- **Record Video** – Record video to a selected storage.
- **Send Images** – Send images to a recipient.
- **Send Notifications** – Send a notification message to a recipient.
- **Send Video Clip** – Send a video clip to a recipient.

Setting Up an Action Rule

An action rule defines the conditions that must be met for the product to perform an action, for example record video or send an email notification. If multiple conditions are defined, all of them must be met to trigger the action.

The following example describes how to set up an action rule to record video to a network share if there is movement in the camera's field of view.

Set up motion detection and add a network share:

1. Go to **Detectors > Motion Detection** and configure a motion detection window. See *page 34*
2. Go to **System Options > Storage** and set up the network share. See *page 54*.

Set up the action rule:

Events

1. Go to **Events** > **Action Rules** and click **Add**.
2. Select **Enable rule** and enter a descriptive name for the rule.
3. Select **Detectors** from the **Trigger** drop-down list.
4. Select **Motion Detection** from the drop-down list. Select the motion detection window to use.
5. Optionally, select a **Schedule** and **Additional conditions**. See below.
6. Under **Actions**, select **Record Video** from the **Type** drop-down list.
7. Select a **Stream profile** and configure the **Duration** settings as described below.
8. Select Network Share from the **Storage** drop-down list.

To add additional criteria, select the **Additional conditions** option and add additional triggers. To prevent an action from being triggered repeatedly, a **Wait at least** time can be set. Enter the time in hours, minutes and seconds, during which the trigger should be ignored before the action rule can be activated again.

The recording **Duration** of some actions can be set to include time immediately before and after the event. Select **Pre-trigger time** and/or **Post-trigger time** and enter the number of seconds. When **While the rule is active** is enabled and the action is triggered again during the post-trigger time, the recording time will be extended with another post-trigger time period.

For more information, see the online help .

Fallback Action

A fallback action is started if the primary action cannot be started, for example if connection to a recipient cannot be established.

Fallback actions are typically used to send email notifications on failed actions or to upload images to a secondary recipient.

Recipients

Recipients receive media files and notification messages. The following recipients are available:

Recipient	Use with action
Email[1]	Send Images Send Notification Send Video Clip
FTP	Send Images Send Video Clip
HTTP	Send Images Send Notification Send Video Clip
HTTPS	Send Images Send Notification Send Video Clip

Events

Network Share[2]	Send Images Send Video Clip
TCP	Send Notification

1. Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.
2. A network share can also be used as a storage device for recorded video. Go **System Options > Storage** to configure a network share before setting up a continuous recording or an action rule to record video. See *Storage, on page 53* for more information about storage devices.

To add a recipient:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a descriptive name.
3. Select a recipient **Type**.
4. Enter the information needed for the recipient type.
5. Click **Test** to test the connection to the recipient.
6. Click **OK**.

Setting Up an Email Recipient

Email recipients can be configured by selecting one of the listed email providers, or by specifying the SMTP server, port and authentication used by, for example, a corporate email server.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.

To set up an email recipient using one of the listed providers:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a **Name** and select **Email** from the **Type** list.
3. Enter the email addresses to send emails to in the **To** field. Use commas to separate multiple addresses.
4. Select the email provider from the **Provider** list.
5. Enter the user ID and password for the email account.
6. Click **Test** to send a test email.

To set up an email recipient using for example a corporate email server, follow the instructions above but select **User defined** as **Provider**. Enter the email address to appear as sender in the **From** field. Select **Advanced settings** and specify the SMTP server address, port and authentication method. Optionally, select **Use encryption** to send emails over an encrypted connection. The server certificate can be validated using the certificates available in the Axis product. For information on how to upload certificates, see *Certificates, on page 47*.

Schedules

Schedules can be used as action rule triggers or as additional conditions, for example to record video if motion is detected outside office hours. Use one of the predefined schedules or create a new schedule as described below.

To create a new schedule:

1. Go to **Events > Schedules** and click **Add**.

2. Enter a descriptive name and the information needed for a daily, weekly, monthly or yearly schedule.
3. Click **OK**.

To use the schedule in an action rule, select the schedule from the **Schedule** drop-down list in the Action Rule Setup page.

Recurrences

Recurrences are used to trigger action rules repeatedly, for example every 5 minutes or every hour.

To set up a recurrence:

1. Go to **Events > Recurrences** and click **Add**.
2. Enter a descriptive name and recurrence pattern.
3. Click **OK**.

To use the recurrence in an action rule, first select **Time** from the **Trigger** drop-down list in the Action Rule Setup page and then select the recurrence from the second drop-down list.

To modify or remove recurrences, select the recurrence in the **Recurrences List** and click **Modify** or **Remove**.

Recordings

Recordings

The Axis product can be configured to record video continuously or according to an action rule:

- To start a continuous recording, see *page 44*.
- To set up action rules, see *page 40*.
- To access recordings, see *Recording List, on page 44*.
- To configure camera controlled storage, see *Storage, on page 53*.

Recording List

Recorded videos are listed on the **Recordings > List** page. The list shows each recording's start date and time, duration and the event that triggered the recording.

To play or download a recording, follow these steps:

1. Go to **Recordings > List**.
2. Use the filter to narrow the list of recordings. Enter the desired filter criteria and click **Filter**. Some filters may take a long time to complete.
3. Select the recording.
4. Click **Play** to play the recording, or click **Download** to download the recording.

Multiple recordings can be downloaded at the same time. Select the recordings and click **Download**. The downloaded file is a zip file containing a minimum of three files, of which the Matroska (mkv) files are the actual recordings. The recordings are time-stamped with the date and time they were downloaded (that is, not the date the recordings were made).

Note

To play recordings in Windows Media Player, AXIS Matroska File Splitter must be installed. AXIS Matroska File Splitter can be downloaded from www.axis.com/techsup/software

For detailed recording and video information, select a recording and click **Properties**.

To remove a recording, select the recording and click **Remove**.

Continuous Recording

The Axis product can be configured to continuously save video to a storage device. See *Storage, on page 53* for more information about storage devices. To prevent the disk from becoming full, it is recommended to configure the disk to automatically remove old recordings. If a new stream profile is selected while a recording is ongoing, the recording will be stopped and saved in the recording list and a new recording with the new stream profile will start. All previous continuous recordings will remain in the recording list until they are removed manually or through automatic removal of old recordings.

To start a continuous recording, follow these steps:

1. Go to **Recordings > Continuous**.
2. Select **Enabled**.
3. Select type of storage device from the **Disk** list.
4. Select a **Stream profile** to use for continuous recordings.
5. Click **Save** to save and start the recording.

Languages

Languages

Multiple languages can be installed in the Axis product. All web pages including the online help will be displayed in the selected language. To switch languages, go to **Setup** > **Languages** and first upload the new language file. Browse and locate the file and click the **Upload Language** button. Select the new language from the list and click Save.

Note

- Resetting the product to factory default settings will erase any uploaded language file and reset the product language to English.
- Clicking the **Restore** button on the Maintenance page will not affect the language.
- A firmware upgrade will not affect the language used. However if you have uploaded a new language to the product and later upgrade the firmware, it may happen that the translation no longer matches the product's web pages. In this case, upload an updated language file.
- A language already installed in the product will be replaced when a current or a later version of the language file is uploaded.

System Options

System Options

Security

Users

User access control is enabled by default and can be configured under **System Options > Security > Users**. An administrator can set up other users by giving them user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page.

The user list displays authorized users and user groups (access levels):

Viewer – Access to the Live View page

Operator – Access to the Live View page and to all settings except System Options

Administrator – Unrestricted access to all settings; can add, modify and remove other users.

Under **HTTP/RTSP Password Settings**, select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you upgraded the firmware and existing clients support encryption but need to log in again and be configured to use this functionality.

Under **User Settings**, select the **Enable anonymous viewer login** option to allow anonymous users access to the Live View page.

Select the **Enable anonymous PTZ control login** to allow anonymous users access to the PTZ controls.

Deselect the **Enable Basic Setup** option to hide the Basic Setup menu. Basic Setup provides quick access to settings that should be made before using the Axis product.

ONVIF

ONVIF (Open Network Video Interface Forum) is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperablity between different vendor products, increased flexibility, reduced cost and future-proof systems.

By creating a user you automatically enable ONVIF communication. Use the user name and password with all ONVIF communication with the product. For more information see *www.onvif.org*

IP Address Filter

IP address filtering is enabled on the **System Options > Security > IP Address Filter** page. Once enabled, the listed IP address are allowed or denied access to the Axis product. Select **Allow** or **Deny** from the list and click **Apply** to enable IP address filtering.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol providing encrypted browsing. HTTPS can also be used by users and clients to verify that the correct device is being accessed. The security level provided by HTTPS is considered adequate for most commercial exchanges.

The Axis product can be configured to require HTTPS when users from different user groups (administrator, operator, viewer) connect.

To use HTTPS, an HTTPS certificate must first be installed. Go to **System Options > Security > Certificates** to install and manage certificates. See *Certificates, on page 47*.

To enable HTTPS on the Axis product:

1. Go to **System Options > Security > HTTPS**

2. Select an HTTPS certificate from the list of installed certificates.
3. Optionally, click **Ciphers** and select the encryption algorithms to use for SSL.
4. Set the **HTTPS Connection Policy** for the different user groups.
5. Click **Save** to enable the settings.

To access the Axis product via the desired protocol, enter `https://` or `http://` in the address field in a browser.

The HTTPS port can be changed on the **System Options > Network > TCP/IP > Advanced** page.

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1X, devices must be authenticated. The authentication is performed by an authentication server, typically a **RADIUS server**, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

In Axis implementation, the Axis product and the authentication server identify themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by a **Certification Authority** (CA). You need:

- a CA certificate to authenticate the authentication server.
- a CA-signed client certificate to authenticate the Axis product.

To create and install certificates, go to **System Options > Security > Certificates**. See *Certificates, on page 47*. Many CA certificates are preinstalled.

To allow the product to access a network protected by IEEE 802.1X:

1. Go to **System Options > Security > IEEE 802.1X**.
2. Select a **CA Certificate** and a **Client Certificate** from the lists of installed certificates.
3. Under **Settings**, select the EAPOL version and provide the EAP identity associated with the client certificate.
4. Check the box to enable IEEE 802.1X and click **Save**.

Note

For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time, on page 48*.

Certificates

Certificates are used to authenticate devices on a network. Typical applications include encrypted web browsing (HTTPS), network protection via IEEE 802.1X and secure upload of images and notification messages for example via email. Two types of certificates can be used with the Axis product:

Server/Client certificates – To authenticate the Axis product.

CA certificates – To authenticate peer certificates, for example the certificate of an authentication server in case the Axis product is connected to an IEEE 802.1X protected network.

Note

Installed certificates, except preinstalled CA certificates, will be deleted if the product is reset to factory default. Preinstalled CA certificates that have been deleted will be reinstalled.

A **Server/Client** certificate can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.

System Options

To install a self-signed certificate:

1. Go to **Setup > System Options > Security > Certificates**.
2. Click **Create self-signed certificate** and provide the requested information.

To create and install a CA-signed certificate:

1. Create a self-signed certificate as described above.
2. Go to **Setup > System Options > Security > Certificates**.
3. Click **Create certificate signing request** and provide the requested information.
4. Copy the PEM-formatted request and send to the CA of your choice.
5. When the signed certificate is returned, click **Install certificate** and upload the certificate.

Server/Client certificates can be installed as **Certificate from signing request** or as **Certificate and private key**. Select **Certificate and private key** if the private key is to be upload as a separate file or if the certificate is in PKCS#12 format.

The Axis product is shipped with several preinstalled **CA certificates**. If required, additional CA certificates can be installed:

1. Go to **Setup > System Options > Security > Certificates**.
2. Click **Install certificate** and upload the certificate.

Date & Time

The Axis product's date and time settings are configured under **System Options > Date & Time**.

Current Server Time displays the current date and time (24h clock). The time can be displayed in 12h clock in the text overlay (see below).

To change the date and time settings, select the preferred **Time mode** under **New Server Time**:

- **Synchronize with computer time** – Sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.
- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration, on page 51*.

  If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration, on page 50*.
- **Set manually** – Allows you to manually set date and time.

If using an NTP server, select your **Time zone** from the drop-down list. If required, check **Automatically adjust for daylight saving time changes**.

The **Date & Time Format Used in Images** is the date and time format displayed as a text overlay in the video stream. Use the predefined formats or see *File Naming & Date/Time Formats* in the online help for information on how to create custom date and time formats. To include date and time in the overlay text, go to **Video** and select **Include date** and **Include time**.

Network

Basic TCP/IP Settings

The Axis product supports IP version 4 and IP version 6. Both versions can be enabled simultaneously, and at least one version must always be enabled.

System Options

IPv4 Address Configuration

By default, the Axis product is set to use IPv4 (IP version 4) and to obtain the IP address automatically via DHCP. The IPv4 settings are configured under **System Options > Network > TCP/IP > Basic**.

DHCP (Dynamic Host Configuration Protocol) allows network administrators to centrally manage and automate the assignment of IP addresses. DHCP should only be enabled if using dynamic IP address notification, or if the DHCP can update a DNS server. It is then possible to access the Axis product by name (host name).

If DHCP is enabled and the product cannot be accessed, run AXIS IP Utility to search the network for connected Axis products, or reset the product to the factory default settings (see *page 57*) and then perform the installation again.

To use a static IP address, check **Use the following IP address** and specify the IP address, subnet mask and default router.

IPv6 Address Configuration

If IPv6 (IP version 6) is enabled, the Axis product will receive an IP address according to the configuration in the network router.

To enable IPv6, go to **System Options > Network > TCP/IP > Basic**. Other settings for IPv6 should be configured in the network router.

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign IP Address Using ARP/Ping, on page 49*.

The ARP/Ping service is enabled by default but is automatically disabled two minutes after the product is started, or as soon as an IP address is assigned. To re-assign IP address using ARP/Ping, the product must be restarted to enable ARP/Ping for an additional two minutes.

To disable the service, go to **System Options > Network > TCP/IP > Basic** and clear the option **Enable ARP/Ping setting of IP address**.

Pinging the product is still possible when the service is disabled.

Assign IP Address Using ARP/Ping

The product's IP address can be assigned using ARP/Ping. The command must be issued within 2 minutes of connecting power.

1. Acquire a free static IP address on the same network segment as the computer.
2. Locate the serial number (S/N) on the product label.
3. Open a command prompt and enter the following commands:

   Linux/Unix syntax

   ```
   arp -s <IP address> <serial number> temp
   ping -s 408 <IP address>
   ```

   Linux/Unix example

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Windows syntax (this may require that you run the command prompt as an administrator)

   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```

   Windows example (this may require that you run the command prompt as an administrator)

   ```
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125
   ```

4. Check that the network cable is connected and then restart the product by disconnecting and reconnecting power.

5. Close the command prompt when the product responds with `Reply from 192.168.0.125:...` or similar.
6. Open a browser and type `http://<IP address>` in the Location/Address field.

For other methods of assigning the IP address, see the Installation and Management Software CD or the document *Assign an IP Address and Access the Video Stream* on Axis Support web at www.axis.com/techsup

Note

- To open a command prompt in Windows, open the **Start menu** and type `cmd` in the **Run/Search** field.
- To use the ARP command in Windows 7/Windows Vista, right-click the command prompt icon and select **Run as administrator**.
- To open a command prompt in Mac OS X, open the **Terminal utility** from **Application > Utilities**.

AXIS Video Hosting System (AVHS)

AVHS used in conjunction with an AVHS service, provides easy and secure Internet access to live and recorded video accessible from any location. For more information and help to find a local AVHS Service Provider go to www.axis.com/hosting

The AVHS settings are configured under **System Options > Network > TCP IP > Basic**. The possibility to connect to an AVHS service is enabled by default. To disable, clear the **Enable AVHS** box.

One-click enabled – Press the product's control button (see *Hardware Overview, on page 6*) to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

Always – The Axis product will constantly attempt to connect to the AVHS service over the Internet. Once registered the product will stay connected to the service. This option can be used when the product is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assigns a host name for easy access to the product. For more information, see *www.axiscam.net*

To register the Axis product with AXIS Internet Dynamic DNS Service, go to **System Options > Network > TCP/IP > Basic**. Under **Services**, click the AXIS Internet Dynamic DNS Service **Settings** button (requires access to the Internet). The domain name currently registered at AXIS Internet Dynamic DNS service for the product can at any time be removed.

Note

AXIS Internet Dynamic DNS Service requires IPv4.

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses. The DNS settings are configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain DNS server address via DHCP** to use the DNS settings provided by the DHCP server.

To make manual settings, select **Use the following DNS server address** and specify the following:

Domain name – Enter the domain(s) to search for the host name used by the Axis product. Multiple domains can be separated by semicolons. The host name is always the first part of a fully qualified domain name, for example, `myserver` is the host name in the fully qualified domain name `myserver.mycompany.com` where `mycompany.com` is the domain name.

Primary/Secondary DNS server – Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and will be used if the primary is unavailable.

System Options

NTP Configuration

NTP (Network Time Protocol) is used to synchronize the clock times of devices in a network. The NTP settings are configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain NTP server address via DHCP** to use the NTP settings provided by the DHCP server.

To make manual settings, select **Use the following NTP server address** and enter the host name or IP address of the NTP server.

Host Name Configuration

The Axis product can be accessed using a host name instead of an IP address. The host name is usually the same as the assigned DNS name. The host name is configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain host name via IPv4 DHCP** to use host name provided by the DHCP server running on IPv4.

Select **Use the host name** to set the host name manually.

Select **Enable dynamic DNS updates** to dynamically update local DNS servers whenever the Axis product's IP address changes.

For more information, see the online help .

Link-Local IPv4 Address

Link-Local Address is enabled by default and assigns the Axis product an additional IP address which can be used to access the product from other hosts on the same segment on the local network. The product can have a Link-Local IP and a static or DHCP-supplied IP address at the same time.

This function can be disabled under **System Options > Network > TCP/IP > Advanced**.

HTTP

The HTTP port used by the Axis product can be changed under **System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 80, any port in the range 1024–65535 can be used.

HTTPS

The HTTPS port used by the Axis product can be changed under **System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 443, any port in the range 1024–65535 can be used.

To enable HTTPS, go to **System Options > Security > HTTPS**. For more information, see *HTTPS, on page 46*.

NAT traversal (port mapping) for IPv4

A network router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (Internet).

Use **NAT traversal** when the Axis product is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the product.

NAT traversal is configured under **System Options > Network > TCP/IP > Advanced**.

Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP™.
- The router has many different names: "NAT router", "Network router", "Internet Gateway", "Broadband router", "Broadband sharing device" or "Home firewall" but the essential purpose of the device is the same.

Enable/Disable – When enabled, the Axis product attempts to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the product (see **System Options > Network > UPnP**).

System Options

Use manually selected NAT router – Select this option to manually select a NAT router and enter the IP address for the router in the field. If no router is specified, the product automatically searches for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port – Select this option to manually define an external HTTP port. Enter the port number in the field. If no port is entered here, a port number is automatically selected when NAT traversal is enabled.

Note

- An alternative HTTP port can be used or be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click **Save**.

FTP

The FTP server running in the Axis product enables upload of new firmware, user applications, etc. The FTP server can be disabled under **System Options > Network > TCP/IP > Advanced**.

Note

This FTP server has nothing to do with the product's ability to transfer images via FTP to other locations and servers.

RTSP

The RTSP server running in the Axis product allows a connecting client to start an H.264 stream. The RTSP port number can be changed under **System Options > Network > TCP/IP > Advanced**. The default port is 554.

Note

H.264 video streams will not be available if the RTSP server is disabled.

SOCKS

SOCKS is a networking proxy protocol. The Axis product can be configured to use a SOCKS server to reach networks on the other side of a firewall or proxy server. This functionality is useful if the Axis product is located on a local network behind a firewall, and notifications, uploads, alarms, etc need to be sent to a destination outside the local network (for example the Internet).

SOCKS is configured under **System Options > Network > SOCKS**. For more information, see the online help .

QoS (Quality of Service)

QoS (Quality of Service) guarantees a certain level of a specified resource to selected traffic on a network. A QoS-aware network prioritizes network traffic and provides a greater network reliability by controlling the amount of bandwidth an application may use.

The QoS settings are configured under **System Options > Network > QoS**. Using DSCP (Differentiated Services Codepoint) values, the Axis product can mark the following types of traffic: live video, event/alarm traffic and management traffic.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

The Axis product can be configured to support SNMP on the **System Options > Network > SNMP** page.

Depending on the level of security required, select the version on SNMP to use.

SNMP v1/v2 provides the lowest level of security. The community name can be specified as a password for read or read/write access to all supported SNMP devices. The default password for the **Read community** is public and the default password for the **Write community** is write.

System Options

Note

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

Traps for SNMP v1/v2 are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

The following traps are available:

- Cold start
- Warm start
- Link up
- Authentication failed

SNMP v3 provides encryption and secure passwords. To use traps with SNMP v3, an SNMP v3 management application is required.

To use SNMP v3, HTTPS must be enabled, see *HTTPS, on page 46*. To enable SNMP v3, check the box and provide the initial user password.

Note

The initial password can only be set once. If the password is lost, the Axis product must be reset to factory default, see *Reset to Factory Default Settings, on page 57*.

UPnP™

The Axis product includes support for UPnP™. UPnP™ is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

UPnP™ can be disabled under **System Options > Network > UPnP™**.

RTP/H.264

The RTP port range and multicast settings are configured under **System Options > Network > RTP**.

The RTP port range defines the range of ports from which the video ports are automatically selected. For multicast streams, only certain IP addresses and port numbers should be used.

Select **Always Multicast Video** to start multicast streaming without opening an RTSP session.

Bonjour

The Axis product includes support for Bonjour. Bonjour is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

Bonjour can be disabled under **System Options > Network > Bonjour**.

Storage

SD Card

The Axis product supports SD cards with up to 64 GB of storage. For best recording performance, use an SDHC or SDXC card with speed class 10.

NOTICE

To prevent corruption of recordings, the SD card should always be unmounted before it is ejected.

The Axis product supports SD cards with the following file systems:

- **ext4** – recommended due to its resilience against data loss if the card is ejected or if there is abrupt power loss. To access data stored on the card from the Windows operating system, a third-party ext4 driver or application is required.
- **vFAT** – most SD cards are pre-formatted with vFAT when purchased.

If required, the SD card can be manually formatted to the desired file system. To format the SD card:

1. Insert the SD card in the SD card slot.
2. Go to **System Options > Storage** and click **SD Card**.
3. Click **Format** and select the desired file system.

Note

During formatting any previous data stored on the disk will be lost.

Mounting is done automatically when the card is inserted or when the product is started. A manual mount is only required if the card has been unmounted and not ejected and re-inserted.

To unmount the SD card:

1. Go to **System Options > Storage** and click **SD Card**.
2. Click **Unmount**.
3. The card can now be removed.

The SD card is managed on the **System Options > Storage** page. Click **SD Card** to open **Storage Management**.

If the card's status shows as failed, click **Check disk** to see if the problem can be found and then try **Repair**. This option is only available for SD cards with ext4. For SD cards with vFAT, use a card reader or computer to troubleshoot the card.

To avoid filling the card, it is recommended to remove recordings continuously. Under **Recording Settings**, select **Remove recordings older than** and select the number of days or weeks.

To stop writing to the card and protect recordings from being removed, select **Lock** under **Recording Settings**.

Network Share

Network share allows you to add network storage such as a NAS (network-attached storage). The NAS shall be dedicated for recordings and data from the Axis products connected to the network. For information about reference NAS devices, go to *www.axis.com/products/cam_companion_software/supported.htm*

To add a network share:

1. Go to **System Options > Storage**.
2. Click **Network Share**.
3. Enter the IP address, DNS or Bonjour name to the host server in the **Host** field.
4. Enter the name of the share in the **Share** field. Sub folders cannot be used.
5. If required, select **The share requires login** and enter the user name and password.
6. Click **Connect**.

To clear all recordings and data from the Axis product's folder on the designated share, click **Clear** under **Storage Tools**.

To avoid filling the share, it is recommended to remove recordings continuously. Under **Recording Settings**, select **Remove recordings older than** and select the number of days or weeks.

To stop writing to the share and protect recordings from being removed, select **Lock** under **Recording Settings**.

System Options

Ports & Devices

I/O Ports

The media converter switch provides two configurable input and output ports for connection of external devices. One port is dedicated for the I/O signals between the media converter switch, the supplied multi-connector cable and the camera. For more information about the multi-connector cable, see *page 58*.

The I/O ports are configured under **System Options > Ports & Devices > I/O Ports**. Select the port direction (**Input** or **Output**). The ports can be given descriptive names and their **Normal states** can be configured as **Open circuit** or **Grounded circuit**.

Port Status

The list on the **System Options > Ports & Devices > Port Status** page shows the status of the product's input and output ports.

Maintenance

The Axis product provides several maintenance functions. These are available under **System Options > Maintenance**.

Click **Restart** to perform a correct restart if the Axis product is not behaving as expected. This will not affect any of the current settings.

Click **Restore** to reset most settings to the factory default values. The following settings are not affected:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the system time
- the IEEE 802.1X settings
- uploaded applications are kept but must be restarted

Click **Default** to reset all settings, including the IP address, to the factory default values. This button should be used with caution. The Axis product can also be reset to factory default using the control button, see *Reset to Factory Default Settings, on page 57*.

To test the product's PTZ mechanics, click **Test** under **PTZ Status**.

For information about firmware upgrade, see *Upgrading the Firmware, on page 59*.

Support

Support Overview

The **System Options > Support > Support Overview** page provides information on troubleshooting and contact information, should you require technical assistance.

See also *Troubleshooting, on page 59*.

System Overview

To get an overview of the Axis product's status and settings, go to **System Options > Support > System Overview**. Information that can be found here includes firmware version, IP address, network and security settings, event settings, image settings and recent log items. Many of the captions are links to the proper Setup page.

System Options

Logs & Reports

The **System Options > Support > Logs & Reports** page generates logs and reports useful for system analysis and troubleshooting. If contacting Axis Support, please provide a valid Server Report with your query.

System Log – Provides information about system events.

Access Log – Lists all failed attempts to access the product. The Access Log can also be configured to list all connections to the product (see below).

Server Report – Provides information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.

Parameter List – Shows the product's parameters and their current settings. This may prove useful when troubleshooting or when contacting Axis Support.

Connection List – Lists all clients that are currently accessing media streams.

Crash Report – Generates an archive with debugging information. The report takes several minutes to generate.

The log levels for the System Log and the Access Log are set under **System Options > Support > Logs & Reports > Configuration**. The Access Log can be configured to list all connections to the product (select Critical, Warnings & Info).

Advanced

Scripting

Scripting allows experienced users to customize and use their own scripts.

NOTICE

Improper use may cause unexpected behavior and loss of contact with the Axis product.

Axis strongly recommends that you do not use this function unless you understand the consequences. Axis Support does not provide assistance for problems with customized scripts.

To open the Script Editor, go to **System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 57*.

For more information, see www.axis.com/developer

File Upload

Files, for example web pages and images, can be uploaded to the Axis product and used as custom settings. To upload a file, go to **System Options > Advanced > File Upload**.

Uploaded files are accessed through `http://<ip address>/local/<user>/<file name>` where `<user>` is the selected user group (viewer, operator or administrator) for the uploaded file.

Plain Config

Plain Config is for advanced users with experience of Axis product configuration. Most parameters can be set and modified from this page. Help is available from the standard help pages.

To open Plain Config, go to **System Options > Advanced > Plain Config**. Axis Support does not provide assistance.

System Options

Reset to Factory Default Settings

Important

Reset to factory default should be used with caution. A reset to factory default will reset all settings, including the IP address, to the factory default values.

Note

The installation and management software tools are available on the CD supplied with the product and from the support pages on *www.axis.com/techsup*

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button and reconnect power. See *Hardware Overview, on page 6*.
3. Keep the control button pressed for about 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is `192.168.0.90`
5. Using the installation and management software tools, assign an IP address, set the password, and access the video stream.

It is also possible to reset parameters to factory default via the web interface. Go to **Setup > System Options > Maintenance**.

Multi-Connector Cable

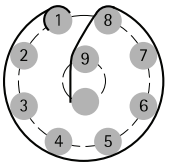
Multi-Connector Cable

The supplied multi-connector cable is required in order to maintain the camera's IP rating.

Connect the multi-connector cable to the camera's multi-connector and to the connectors in the supplied media converter switch, see *page 6*.

The cable provides the following signals:

- DC power to camera
- Network (Ethernet 10/100Base-T)
- Input/Output (I/O)



Function	Pin – wire	Notes	Specifications
Configurable (Input or Output)	2 – blue 7 – yellow	Digital input – Connect to pin 8 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		Digital output – Connected to pin 1 when activated, floating (unconnected) when deactivated. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 30 V DC, open drain, 100 mA
RX+	3 – green/white	Ethernet – receiving	
RX-	4 – green	Ethernet – receiving	
TX+	5 – orange/white	Ethernet – transmitting	
TX-	6 – orange	Ethernet – transmitting	
0 V DC (-)	8 – black		0 V DC
DC output (12 V)	1, 9 – red	Used to power camera	12–13.2 V DC Max load = 6 A

Troubleshooting

Checking the Firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in the Axis product is displayed in the page **Setup > Basic Setup** and in **Setup > About**.

Upgrading the Firmware

When you upgrade the Axis product with the latest firmware from Axis website, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release, before upgrading the firmware.

To upgrade, follow these instructions:

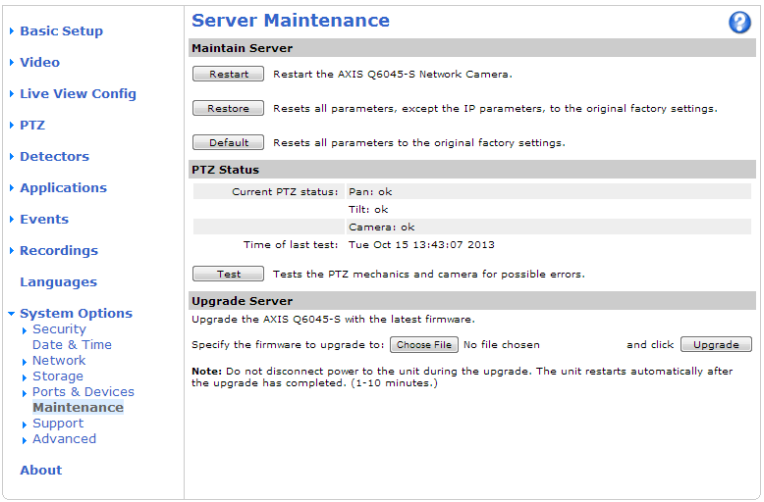
1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from Axis website at *www.axis.com/techsup*
2. Go to **Setup > System Options > Maintenance** in the product's web pages.
3. Under **Upgrade Server**, click **Browse** and locate the file on your computer. Click **Upgrade**.

After starting the upgrade process, always wait at least 5–10 minutes before restarting the product, even if you suspect the upgrade has failed.

AXIS Camera Management can be used for multiple upgrades. See *www.axis.com* for more information.

Note

- Your dealer reserves the right to charge for any repair attributable to faulty upgrade by the user.
- Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.



Emergency Recovery Procedure

If power or network connection is lost during the upgrade, the process fails and the product becomes unresponsive. Flashing red Status indicator indicates a failed upgrade. To recover the product, follow the steps below. The serial number is found on the product's label.

1. In **UNIX/Linux**, type the following from the command line:

Troubleshooting

```
arp -s <IP address> <serial number> temp
ping -l 408 <IP address>
```

In **Windows**, type the following from a command/DOS prompt (this may require that you run the command prompt as an administrator):

```
arp -s <IP address> <serial number>
ping -l 408 -t <IP address>
```

2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the product's IP address. In the page that opens, use the **Browse** button to select the upgrade file to use. Then click **Load** to restart the upgrade process.
4. After the upgrade is complete (1–10 minutes), the product automatically restarts and shows a steady green on the Status indicator.
5. Reinstall the product, referring to the Installation Guide.

If the emergency recovery procedure does not get the product up and running again, contact Axis support at www.axis.com/techsup/

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address	
When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the product. Ensure the Ping length is set to 408. For instructions, see *Assign IP Address Using ARP/Ping, on page 49*.
The product is located on a different subnet	If the IP address intended for the product and the IP address of the computer used to access the product are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	Disconnect the Axis product from the network. Run the Ping command (in a Command/DOS window, type `ping` and the IP address of the product): • If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the product. • If you receive: `Request timed out`, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
Possible IP address conflict with another device on the same subnet.	The static IP address in the Axis product is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the product.

The product cannot be accessed from a browser	
Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type `http` or `https` in the browser's address field. If the password for the user root is lost, the product must be reset to the factory default settings. See *Reset to Factory Default Settings, on page 57*.

Troubleshooting

The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Camera Management to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, see the Installation and Management Software CD or the document *Assign an IP Address and Access the Video Stream* on Axis Support web at www.axis.com/techsup.
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time, on page 48*.

The product is accessible locally but not externally

Router configuration	To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see *NAT traversal (port mapping) for IPv4, on page 51*. The router must support UPnP™.
Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	Check if you need to configure the router settings from **System Options > Network > TCP/IP > Basic**.

Problems with streaming H.264

Problems with AXIS Media Control (*Internet Explorer only*)	To enable the updating of video images in Internet Explorer, set the browser to allow ActiveX controls. Also, make sure that AXIS Media Control is installed on your computer.
No H.264 displayed in the client	Check that the relevant H.264 connection methods and correct interface are enabled in the AMC Control Panel (streaming tab). See *AXIS Media Control (AMC), on page 16*. In the AMC Control Panel, select the H.264 tab and click **Set to default H.264 decoder**. Check that RTSP is enabled under **System Options > Network > TCP/IP > Advanced**.
Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the product need to be configured. The TTL (Time To Live) value may need to be increased.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the Axis product are valid for your network. Check with your network administrator to see if there is a firewall preventing viewing.
Installation of additional ActiveX component restricted or prohibited	Configure the Axis product to use a Java applet for updating video images in your browser. Go to **Setup > Live View Config** and select Java applet under **Default viewer**.
Poor rendering of H.264 images	Ensure that your graphics card is using the latest driver. The latest drivers can usually be downloaded from the manufacturer's website.
Color saturation is different in H.264 and Motion JPEG	Modify the settings for your graphics adapter. Refer to the adapter's documentation for more information.

Troubleshooting

Lower frame rate than expected	See *Performance Considerations, on page 67*. Reduce the number of applications running on the client computer. Limit the number of simultaneous viewers. Check with the network administrator that there is enough bandwidth available. Check in the AMC Control Panel (H.264 tag) that video processing is NOT set to **Decode only key frames**. Lower the image resolution. The maximum frames per second is dependent on the utility frequency (60/50 Hz) of the Axis product. See *Technical Specifications, on page 63*.

Video and image problems, general

Image unsatisfactory	Check the video stream and camera settings under **Setup > Video > Video Stream** and **Setup > Video > Camera Settings**.

Motion Detection triggers unexpectedly

Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may trigger mistakenly. Lower the sensitivity setting to avoid problems with luminance.

Storage and disk management problems

Storage disruption	A storage disruption alarm is sent if a storage device is unavailable, removed, full, locked or if other read or write problems occur. To identify the source of the problem, check the **System Log** under **System Options > Support > Logs & Reports**. Depending on the problem, it might be necessary to re-mount the storage device. For information on how to set up a storage disruption alarm, see *Events, on page 39*.
Video cannot be recorded	Check that the SD card is not write protected (that is, read only).
SD card cannot be mounted	Reformat the SD card and then click Mount.

Media converter switch

Media converter switch freezes after hotswapping	The media converter switch does not support hotswapping. Disconnect power from the switch before swapping cameras. Restart the switch after a failed attempt to hotswap.

Technical Specifications

Technical Specifications

Function/group	Item	Specifications
Camera	Models	AXIS Q6045-S 50 Hz AXIS Q6045-S 60 Hz
	Image sensor	1/3" Progressive Scan CMOS
	Lens	f 4.45 – 89.0 mm F1.6 – 2.9 Autofocus Automatic day/night Horizontal angle of view: 62.98° – 3.49°
	Minimum illumination	Color: 0.6 lux at 30 IRE F1.6 B/W: 0.04 lux at 30 IRE F1.6
	Shutter time	1/33000 s to 1/3 s (50 Hz) 1/33000 s to 1/4 s (60 Hz)
	Pan/Tilt/Zoom	E-flip 256 preset positions Pan 360° endless, 0.05° – 450°/s Tilt: 220°, 0.05° – 450°/s 20x optical zoom and 12x digital zoom, total 240x zoom
	Pan/Tilt/Zoom functionalities	Tour recording, guard tour, control queue On-screen directional indicator, Set new pan 0°
Video	Video compression	H.264 Main and Baseline profile (MPEG-4 Part 10/AVC) Motion JPEG
	Resolutions	1920x1080 HDTV 1080p to 320x180
	Frame rate H.264	Up to 25/30 fps (50/60 Hz)
	Frame rate Motion JPEG	Up to 25/30 fps (50/60 Hz)
	Video streaming	Multiple, individually configurable streams in H.264 and Motion JPEG Controllable frame rate and bandwidth VBR/CBR H.264
	Image settings	Wide Dynamic Range (WDR), manual shutter time, compression, color, brightness, sharpness, white balance, exposure control, exposure zones, rotation, backlight compensation, highlight compensation, fine tuning of behavior at low light Text and image overlay 32 individual 3D privacy masks Image freeze on PTZ
Network	Security	Password protection, IP address filtering, HTTPS encryption*, IEEE 802.1X network access control*, digest authentication, user access log *This product includes software developed by the Open SSL Project for use in the Open SSL Toolkit (www.openssl.org)
	Supported protocols	IPv4/v6, HTTP, HTTPS*, SSL/TLS*, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH *This product includes software developed by the Open SSL Project for use in the Open SSL Toolkit (www.openssl.org)

Technical Specifications

Function/group	Item	Specifications
System Integration	Application Programming Interface	Open API for software integration, including VAPIX® and AXIS Camera Application Platform from Axis Communications; specifications at www.axis.com AXIS Video Hosting System (AVHS) with One-Click Camera Connection ONVIF Profile S, specification at www.onvif.org
	Intelligent video	Video motion detection, Autotracking, Active Gatekeeper Basic analytics (not to be compared with third-party analytics): Object removed, Enter/Exit detector, Fence detector, Object counter, Highlight compensation Support for AXIS Camera Application Platform enabling installation of additional applications
	Event triggers	Detectors: Live Stream Accessed, Motion Detection, Enter/Exit, Fence Detector, Object Removed Hardware: Casing Open, Fan, Heater, Network, Temperature Input Signal: Manual Trigger, Virtual Inputs PTZ: Autotracking, Error, Moving, Preset Reached, Ready Storage: Disruption, Recording System: System Ready, Shock Detected Time: Recurrence, Use Schedule
	Event actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP External output, PTZ preset, guard tour, video recording to edge storage, autotracking, day/night mode Pre- and post-alarm video buffering
	Installation aid	Pixel counter
	Video access from web browser	Camera live view Video recording to file (ASF) Customizable HTML pages Windows 7, Windows Vista, Windows XP, Windows Server 2008, Windows Server 2003 DirectX 9c or higher For other operating systems and browsers, see www.axis.com/techsup
	Management and maintenance	AXIS Camera Management tool on CD and web-based configuration Configuration of backup and restore Firmware upgrades over HTTP or FTP, firmware available on www.axis.com

Technical Specifications

Function/group	Item	Specifications
General	Casing	IP6K9K-, IP66-, IP67- and NEMA 4X-rated metal casing (stainless steel ASTM 316L/UNS S31603/EN 1.4432), nylon clear dome
	Memory	512 MB RAM, 128 MB Flash Battery backed-up real-time clock
	Power	60 W powered through AXIS T8605 Media Converter Switch
	Connectors	IP-66 rated multi-connector for DC power, Ethernet 10/100Base-T, input and output, including 7 m (23 ft.) cable AXIS T8605 Media Converter Switch: 2x RJ-45 10/100Base-T, 2x SFP 100Base-FX/1000Base-X, terminal blocks with power input, power output and 2x configurable input/output
	Edge storage	Supports SD cards with up to 64 GB of storage. For best recording performance, use an SDHC or SDXC card with speed class 10. (card not included) Support for recording to network share (Network Attached Storage or file server)
	Operating conditions	-30 °C to 50 °C (-22 °F to 122 °F) Humidity 10–100% RH (condensing)
	Storage conditions	-40 °C to 65 °C (-40 °F to 149 °F)
	Approvals	EN 55022 Class A, EN 61000-3-2, EN 61000-3-3, EN 61000-6-1, EN 61000-6-2, EN 55024, EN 50121-4, IEC 62236-4, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, C-tick AS/NZS CISPR 22 Class A, KCC KN22 Class A, KN24, IEC/EN/UL 60950-1, IEC/EN/UL 60950-22, IEC/EN 60529 IP66, IP67, ISO 20653 IP6K9K, NEMA 250 Type 4X, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-78, IEC 60068-2-14, IEC 60068-2-30, IEC 60068-2-6, IEC 60068-2-27, IEC 60068-2-60, MIL-STD 810G 509.5
	Weight	Camera: 5.7 kg (12.6 lb.)
	Included accessories	AXIS T8605 Media Converter Switch, IP66–rated multi-connector cable, Installation Guide, Installation and Management Software CD, Windows decoder 1-user license
	Video management software	AXIS Camera Companion (software included on CD) — Basic surveillance for small businesses, where video is recorded to edge storage AXIS Camera Station (sold separately) — Fully featured surveillance for medium-sized installations, where video is recorded on a system server For more information and software applications from partners, see www.axis.com/products/video/software/
	Optional accessories	Power supply Wall bracket Mounting bracket for T91C (AXIS T91C Mounting Accessories) Smoked dome cover Stainless steel sunshield AXIS T8310 Video Surveillance Control Board AXIS P8221 Network I/O Audio Module AXIS T90A Illuminators Installation Display Multi-user decoder license pack

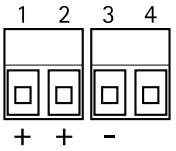
Technical Specifications

Media Converter Switch Connectors

Camera Connectors

Power connector

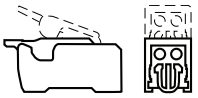
Two 2-pin terminal blocks for power output (pin 4 is not used).



Function		Pin	Notes	Specifications
DC output	12 V DC	1, 2	Power out to camera	Max load = 6.5 A 12.0–13.2 V DC, min 70 W
	0 V DC (-)	3		0 V DC
	N/a	4	N/a	

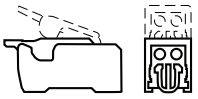
Network connector

Two 2-pin Ethernet terminal blocks.



I/O terminal connector

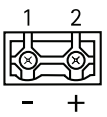
2-pin terminal block.



External Connectors

Power connector

2-pin terminal block for power input.



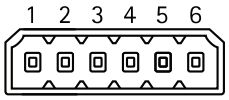
Function		Pin	Notes	Specifications
DC input	0 V DC (-)	1		0 V DC
	12 V DC	2	Power in from power supply (sold separately)	Max load = 7 A 12.0–13.2 V DC, min 75 W

Technical Specifications

I/O terminal connector

6-pin terminal blocks for:

- Digital Input/Output
- Power (DC output)
- 0 V DC (-)



Function	Pin	Notes	Specifications
0 V DC (-)	1, 4, 6		0 V DC
DC output	2	Power out	12 V DC, 50 mA
Configurable I/O 1 (Input or Output)	3	Digital input	0 to max 30 V DC
		Digital output (transistor – open collector)	0 to max 30 V DC, open drain, 100 mA
Configurable I/O 2 (Input or Output)	5	Digital input	0 to max 30 V DC
		Digital output (transistor – open collector)	0 to max 30 V DC, open drain, 100 mA

Performance Considerations

When settings up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

The following factors are among the most important to consider:

- High image resolution and/or lower compression levels result in images containing more data. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression) by different clients. Effect on frame rate and bandwidth.
- Accessing Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affect the product's CPU load. Frame rate affected.
- Heavy network utilization due to poor infrastructure. Bandwidth affected.
- Viewing on poorly performing client computers lowers perceived performance. Frame rate affected.

User Manual
AXIS Q6045–S PTZ Dome Network Camera
© Axis Communications AB, 2014
Ver. M1.7
Date: January 2014
Part No. 54202